

กระบวนการหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนามภายใต้กฎหมายไทย:
ข้อเสนอในการแก้ไขกฎหมาย*

The Procedure for Identifying Anonymous Online Defamers under Thai Law:
A Proposal for Legal Amendment

ชีวิน มัลลิกะมาลย์ **

ภาควิชานิติศาสตร์ คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

Cheewin Mallikamarl

Department of Law, Faculty of Social Sciences, Kasetsart University

วันที่รับบทความ 9 มีนาคม 2569; วันแก้ไขบทความ 20 พฤษภาคม 2569; วันตอบรับบทความ 28 มิถุนายน 2569

บทคัดย่อ

กฎหมายหมิ่นประมาทของประเทศไทยไม่สามารถคุ้มครองสิทธิในชื่อเสียงของผู้เสียหายได้อย่างมีประสิทธิภาพ หากผู้เสียหายถูกหมิ่นประมาททางออนไลน์โดยนิรนาม เพราะผู้เสียหายไม่ทราบว่าใครคือบุคคลที่หมิ่นประมาท ในการหาตัวผู้หมิ่นประมาท ผู้เสียหายต้องอาศัยกระบวนการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไขเพิ่มเติม) จากการวิเคราะห์กระบวนการนี้ บทความนี้พบว่าพนักงานเจ้าหน้าที่ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ มีอำนาจเรียกข้อมูลจากผู้ให้บริการอินเทอร์เน็ตเพื่อระบุตัวผู้กระทำความผิดซึ่งสามารถใช้ในการหาตัวผู้หมิ่นประมาทได้ แต่บทความนี้เห็นว่า กระบวนการนี้มีปัญหาในทางปฏิบัติ เช่น พนักงานเจ้าหน้าที่ ฯ มีจำนวนไม่เพียงพอในการดำเนินคดีหมิ่นประมาท บทความนี้ได้เสนอทางแก้ไขจากการเปรียบเทียบแนวทางของกฎหมายไทยกับแนวทางของกฎหมายสหรัฐอเมริกา ซึ่งให้สิทธิผู้เสียหายร้องขอให้ศาลสั่งให้ผู้ให้บริการอินเทอร์เน็ตเปิดเผยข้อมูลเกี่ยวกับผู้หมิ่นประมาทโดยนิรนามได้โดยตรงตามแนวทางของกฎหมายสหรัฐอเมริกานี้ ศาลต้องชั่งน้ำหนักว่าจะให้ความสำคัญกับสิทธิในชื่อเสียงของผู้เสียหายหรือเสรีภาพในการสื่อสารของผู้ใช้อินเทอร์เน็ตโดยนิรนามมากกว่ากัน เพราะกฎหมายสหรัฐอเมริการับรองการสื่อสารโดยนิรนามในฐานะที่เป็นส่วนหนึ่งของเสรีภาพในการสื่อสารที่ได้รับความคุ้มครองตามรัฐธรรมนูญ บทความนี้จึงได้เสนอให้กฎหมายไทยนำแนวทางนี้มาใช้โดยการแก้ไขเพิ่มเติมมาตรา 18 ของ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ และบทความนี้ยังเห็นว่าแนวทางนี้สามารถแก้ปัญหาทางปฏิบัติข้างต้นได้ เพราะผู้เสียหายสามารถร้องขอต่อศาลยุติธรรมของไทยเพื่อมีคำสั่งให้ผู้ให้บริการอินเทอร์เน็ตเปิดเผยตัวตนของผู้หมิ่นประมาทได้โดยตรง โดยไม่ต้องอาศัยอำนาจของพนักงานเจ้าหน้าที่ ฯ

คำสำคัญ: หมิ่นประมาท, หมิ่นประมาทโดยนิรนาม, การหาตัวผู้กระทำความผิดออนไลน์, พนักงานเจ้าหน้าที่, ผู้ให้บริการ

* บทความนี้เป็นสรุปจากงานวิจัยเรื่อง “การหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนามภายใต้กฎหมายไทย: ข้อเสนอในการแก้ไขเพิ่มเติมพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์”

** อาจารย์ ภาควิชานิติศาสตร์ คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์

ที่อยู่: ภาควิชานิติศาสตร์ คณะสังคมศาสตร์ มหาวิทยาลัยเกษตรศาสตร์ เลขที่ 50 ถนนงามวงศ์วาน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ 10900

E-mail: cheewin.m@ku.th

Abstract

Thailand's defamation law fails to effectively protect the reputational rights of victims who are anonymously defamed online, as they do not know the identities of the defamers. Victims must rely on the procedure outlined in the Computer Crime Act B.E. 2550 (2007) (and its amendments) ('CCA') to identify the defamers. Having analysed the Act, this article shows that competent officials can request information from Internet Service Providers (ISPs) to identify perpetrators. This procedure can be applied to identify anonymous online defamers. However, the article argues that the procedure has practical problems such as insufficient numbers of competent officials to handle online defamation cases. To provide a solution, this article compares the Thai approach with the approach under US law, which allows defamed victims to directly request a court to order ISPs to reveal the identities of the anonymous defamers. Under the US approach, the court must weigh whether to prioritise the victim's right to reputation or the anonymous user's right to free speech. This is because US law recognises anonymous speech as an aspect of free speech protected by the Constitution. This article, therefore, proposes that Thai law should adopt this approach by amending Section 18 of the CCA. It also argues that the US approach can solve the practical problems under Thai law because defamed victims can directly request the Thai Court of Justice to order ISPs to reveal their anonymous defamers' identities without having to rely on the competent officials.

Keywords: Defamation, Anonymous Defamation, Identification of Online Perpetrators, Competent Official, Service Providers

1. บทนำ

ปัจจุบันการหมิ่นประมาทผู้อื่นเป็นความผิดอาญาตามประมวลกฎหมายอาญามาตรา 326¹ และการหมิ่นประมาทนั้นทำให้สาธารณชนรับทราบข้อความได้ ผู้หมิ่นประมาทต้องรับโทษฐานหมิ่นประมาทโดยการโฆษณาตามมาตรา 328² ทั้งนี้ กฎหมายไทยไม่ได้มีการแบ่งแยกความผิดฐานหมิ่นประมาทโดยทั่วไปกับการหมิ่นประมาททางออนไลน์ (Online Defamation)³ นอกจากการหมิ่นประมาทจะเป็นความผิดตามประมวลกฎหมายอาญาแล้ว ผู้เสียหายที่ถูกหมิ่นประมาทสามารถเรียกร้องค่าสินไหมทดแทนโดยอาศัยประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 423 วรรคแรก⁴ มาตรา 420⁵ และมาตรา 447⁶ ได้ กฎหมายที่กล่าวมานี้มุ่งคุ้มครองสิทธิในชื่อเสียงของบุคคลซึ่งเป็นสิทธิที่ได้รับการรับรองตามรัฐธรรมนูญแห่งราชอาณาจักรไทย⁷

นอกจาก กฎหมายคุ้มครองสิทธิในชื่อเสียงแล้ว ประมวลกฎหมายทั้งสองฉบับยังมีบทบัญญัติที่รับรองเสรีภาพในการแสดงออก หรือเสรีภาพในการสื่อสารของผู้ที่ถูกกล่าวหาว่าหมิ่นประมาทผู้อื่นด้วย เสรีภาพนี้ได้รับการรับรองตามรัฐธรรมนูญแห่งราชอาณาจักรไทยเช่นกัน⁸ ตามกฎหมายอาญา บุคคลที่ถูกฟ้องว่าหมิ่นประมาทสามารถอ้างว่า ตนแสดงความเห็นโดยสุจริตตามประมวลกฎหมายอาญามาตรา 329⁹ หรืออ้างว่า ข้อความที่ตนเองหมิ่นประมาทเป็นความจริง และการพิสูจน์ว่าเป็นความจริงนั้นเป็นประโยชน์ต่อสาธารณชนตามประมวลกฎหมายอาญามาตรา 330¹⁰ ตามกฎหมายแพ่ง บุคคลที่ถูกฟ้องเรียกค่าสินไหมทดแทนจากการหมิ่นประมาทผู้อื่นสามารถอ้างข้อยกเว้นความรับผิด โดยอาศัยมาตรา 423 วรรคสองได้¹¹ หรือสามารถนำข้อยกเว้นทางอาญามาปฏิเสธความรับผิดทางแพ่งได้เช่นกัน¹²

การดำเนินคดีกับบุคคลที่หมิ่นประมาท ผู้เสียหายสามารถดำเนินคดีอาญาโดยฟ้องคดีด้วยตนเองได้¹³ หรือ ร้องทุกข์ต่อพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา¹⁴ เพื่อดำเนินการตามกฎหมายวิธีพิจารณาความอาญา โดยให้พนักงานอัยการเป็นผู้ฟ้องคดีแทนผู้เสียหาย ในกรณีที่ผู้เสียหายต้องการเรียกค่าสินไหมทดแทนตามกฎหมายแพ่งจากผู้หมิ่นประมาท ผู้เสียหายสามารถฟ้องเป็นคดีแพ่งได้

¹ ประมวลกฎหมายอาญา มาตรา 326.

² ประมวลกฎหมายอาญา มาตรา 328.

³ ก่อนปี 2560 พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 14(1) ถูกตีความว่าเป็นบทบัญญัติที่ลงโทษบุคคลที่หมิ่นประมาททางออนไลน์ เช่น ในคำพิพากษาฎีกาเลขที่ 3334/2558 แต่ในปี 2560 ได้มีการแก้ไขเพิ่มเติม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ฯ โดยระบุว่า มาตรา 14(1) ไม่รวมการกระทำความผิดฐานหมิ่นประมาทตามประมวลกฎหมายอาญา...” การหมิ่นประมาทออนไลน์จึงไม่เป็นความผิดตามมาตรา 14(1) พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ฯ อีกต่อไป.

⁴ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 423.

⁵ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 420 โปรดดูตัวอย่าง คำพิพากษาฎีกาที่ 891/2557.

⁶ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 447.

⁷ รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 32.

⁸ รัฐธรรมนูญแห่งราชอาณาจักรไทย มาตรา 34.

⁹ ประมวลกฎหมายอาญา มาตรา 329.

¹⁰ ประมวลกฎหมายอาญา มาตรา 330.

¹¹ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 423 วรรคสอง.

¹² คำพิพากษาฎีกาที่ 1972/2517.

¹³ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 28(2).

¹⁴ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 123.

นอกจากนี้ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 44/1¹⁵ ยังให้สิทธิผู้เสียหายในคดีหมิ่นประมาทยื่นคำร้อง เพื่อขอให้พนักงานอัยการเรียกค่าสินไหมทดแทนในความเสียหายที่เกิดขึ้นกับชื่อเสียงแทนได้ด้วย

หลักกฎหมายที่กล่าวมาทำให้เห็นว่า ในปัจจุบันกฎหมายไทยได้พยายามสร้างความสมดุล (Balance) ระหว่างการคุ้มครองสิทธิในชื่อเสียงของผู้เสียหาย และเสรีภาพในการสื่อสารของผู้หมิ่นประมาท กล่าวคือ บุคคลที่ทำให้ผู้อื่นเสียชื่อเสียงอาจไม่ต้องรับโทษทางอาญาหรือรับผิดทางแพ่ง หากบุคคลนั้นอ้างว่าการกระทำของตนเป็นกระทำโดยชอบตามหลักประมวลกฎหมายอาญา มาตรา 329, 330 หรือ ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 423 วรรคสอง แม้กฎหมายได้พยายามสร้างความสมดุลระหว่างการคุ้มครองสิทธิในชื่อเสียงและเสรีภาพในการสื่อสาร แต่ผู้วิจัยจะนำเสนอในบทความวิจัยนี้ว่า ปัจจุบันกฎหมายไทยยังไม่สามารถให้ความคุ้มครองสิทธิในชื่อเสียงของบุคคลได้อย่างมีประสิทธิภาพ เนื่องจากการสื่อสารโดยใช้สื่อออนไลน์มีลักษณะพิเศษ คือ ผู้สื่อสารสามารถใช้นามแฝง (Pseudonym) หรือ ปิดบังตนเอง (Anonymous) ขณะสื่อสารได้ รองศาสตราจารย์ศณานิธิ ทองรวีวงศ์ เรียกการสื่อสารเช่นนี้ว่า “การสื่อสารข้อมูลออนไลน์โดยนิรนาม”¹⁶ การสื่อสารเช่นนี้อาจนำไปสู่การทำผิดเกี่ยวกับคอมพิวเตอร์โดยอาศัยความนิรนามเป็นปัจจัยก่อเหตุ เช่น การฉ้อโกงออนไลน์ การคุกคามออนไลน์ การกลั่นแกล้งออนไลน์ รวมไปถึงการหมิ่นประมาทออนไลน์ด้วย¹⁷ เนื่องจากการสื่อสารโดยนิรนามเป็นการปิดบังตัวเอง บุคคลที่ทำผิดกฎหมายหรือละเมิดสิทธิของผู้อื่นจึงใช้การสื่อสารเช่นนี้ เพื่อหลีกเลี่ยงการถูกดำเนินคดี¹⁸ การสื่อสารเช่นนี้ ย่อมเป็นอุปสรรคต่อผู้เสียหายที่ถูกหมิ่นประมาทโดยนิรนามในการใช้สิทธิตามกฎหมาย เพื่อคุ้มครองชื่อเสียงของตนเพราะผู้เสียหายไม่ทราบว่าต้องดำเนินคดีกับใคร

แม้การสื่อสารทางออนไลน์จะเปิดโอกาสให้ผู้สื่อสารกระทำโดยนิรนามได้ แต่ทุกคนที่สื่อสารทางออนไลน์จำเป็นต้องใช้บริการของ “ตัวกลางทางอินเทอร์เน็ต (Internet Intermediaries)” ทั้งนี้ องค์การเพื่อความร่วมมือทางเศรษฐกิจและการพัฒนา (Organisation for Economic Co-operation and Development: OECD) ได้อธิบายว่า “บุคคลใช้ตัวกลางทางอินเทอร์เน็ตในการติดต่อสื่อสารระหว่างกัน หรือใช้ตัวกลางนี้เพื่อความสะดวกในการทำธุรกรรมต่าง ๆ ทางอินเทอร์เน็ต บุคคลใช้ตัวกลางทางอินเทอร์เน็ตเพื่อเข้าถึง จัดเก็บ ส่งต่อ หรือ ระบุเนื้อหา สินค้า หรือ บริการ ที่อยู่ในอินเทอร์เน็ตของบุคคลอีกฝ่ายหนึ่งได้”¹⁹ สำหรับตัวอย่างของตัวกลางทางอินเทอร์เน็ต เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service and Access Providers) ซึ่งทำให้ผู้ใช้บริการสามารถเข้าสู่ระบบอินเทอร์เน็ตได้ หรือ ผู้ให้บริการเครือข่ายสังคมที่ให้พื้นที่แก่ผู้ใช้บริการในการแสดงออกซึ่งความคิด²⁰

ประเทศไทยได้กำหนดกระบวนการในการหาตัวผู้กระทำผิดทางออนไลน์ที่ใช้การสื่อสารโดยนิรนาม เพื่อหลีกเลี่ยงการถูกดำเนินคดี โดยบัญญัติกระบวนการไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (และที่แก้ไขเพิ่มเติม) (‘พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ’) กฎหมาย

¹⁵ ประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 44/1 โปรดดูตัวอย่างคำพิพากษาฎีกาเลขที่ 4403/2566.

¹⁶ ศณานิธิ ทองรวีวงศ์, ‘สิทธิในการสื่อสารข้อมูลออนไลน์โดยนิรนามของพลเมือง’ (2558) 8(2) วารสารนิติสังคมศาสตร์ 72.

¹⁷ เฟื่องอ้าง 90-91.

¹⁸ ตัวอย่างข้อเท็จจริงที่มีการใช้การสื่อสารโดยนิรนามในการหมิ่นประมาทผู้อื่น เช่น ‘กามิน แจ้งความตำรวจไซเบอร์ เอาผิดเว็บไซต์-เพจอวดตาร’ (One31, 28 มีนาคม 2568) <<https://www.one31.net/news/detail/74614>> สืบค้นวันที่ 11 สิงหาคม 2568.

¹⁹ OECD, ‘The Role of Internet Intermediaries in Advancing Public Policy Objectives’ (OECD Publishing 2011) 20.

²⁰ ibid 21.

ฉบับนี้เรียก “ตัวกลางทางอินเทอร์เน็ต” ว่า “ผู้ให้บริการ”²¹ และกำหนดให้ผู้ให้บริการนี้ มีหน้าที่ส่งข้อมูลให้พนักงานเจ้าหน้าที่ซึ่งได้รับการแต่งตั้งให้ปฏิบัติหน้าที่ตามกฎหมายฉบับนี้²² (‘พนักงานเจ้าหน้าที่ ฯ’)

ในบทความนี้ ผู้วิจัยได้อธิบายการนำกระบวนการข้างต้นมาใช้ในการระบุตัวผู้หมิ่นประมาทโดยนิรนามทางออนไลน์ (Online Anonymous Defamers) โดยใช้วิธีวิเคราะห์หลักกฎหมาย (Doctrinal Research Method) ซึ่งคือ กระบวนการวิจัยที่ใช้ในการระบุ วิเคราะห์ และสังเคราะห์เนื้อหาของกฎหมาย²³ โดยมุ่งไปที่บทบัญญัติของ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ เป็นหลัก เพราะเป็นกฎหมายที่ใช้ในการหาตัวผู้กระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำ โดยผู้วิจัยนำงานวิชาการที่เกี่ยวข้องกับ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ และคำพิพากษากฎีกาวิเคราะห์ เพื่อแสดงให้เห็นถึงกระบวนการปัจจุบันที่ใช้ในการหาตัวผู้หมิ่นประมาทโดยนิรนาม

นอกจากการนำเสนอกระบวนการหาตัวผู้หมิ่นประมาทแล้ว ผู้วิจัยได้วิเคราะห์งานวิชาการที่เกี่ยวข้องกับการบังคับใช้ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ เพื่อนำเสนอว่า กระบวนการนี้ในทางปฏิบัติมีอุปสรรคในการหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนาม เพราะ (1) ผู้ให้บริการที่ต้องส่งข้อมูลให้พนักงานเจ้าหน้าที่ ฯ อาจไม่ให้ความร่วมมือในการระบุตัวผู้หมิ่นประมาท และ (2) พนักงานเจ้าหน้าที่ซึ่งมีอำนาจในการดำเนินคดีตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ มีจำนวนไม่มากอันเป็นอุปสรรคต่อการหาตัวผู้หมิ่นประมาท นอกจากนี้ กระบวนการนี้เกิดคำถามทางกฎหมายว่า การหาตัวผู้กระทำความผิดถือเป็นการละเมิดสิทธิความเป็นอยู่ส่วนตัวของผู้หมิ่นประมาทเกินสมควรหรือไม่

เพื่อแก้ไขปัญหาก็กล่าวมาข้างต้น ผู้วิจัยได้ทำการศึกษาแนวทางของกฎหมายสหรัฐอเมริกาเกี่ยวกับการหาตัวผู้หมิ่นประมาทโดยนิรนาม เพราะการดำเนินคดีหมิ่นประมาททางออนไลน์ตามกฎหมายสหรัฐอเมริกาต้องดำเนินคดีกับผู้หมิ่นประมาทโดยตรง²⁴ โดยผู้เสียหายมีสิทธิในการร้องขอให้ศาลมีคำสั่งให้ผู้ให้บริการอินเทอร์เน็ตเปิดเผยตัวผู้ใช้อินเทอร์เน็ตโดยนิรนามได้ ทั้งนี้ ในการพิจารณาว่าจะมีคำสั่งให้เปิดเผยตัวหรือไม่ ศาลต้องชั่งน้ำหนักระหว่างการคุ้มครองสิทธิในชื่อเสียงกับสิทธิในการสื่อสารโดยนิรนามซึ่งศาลสูงสุดของประเทศสหรัฐอเมริกา (The Supreme Court of the United States of America) เคยรับรองว่าสิทธิในการสื่อสารโดยนิรนามถือเป็นส่วนหนึ่งของเสรีภาพในการสื่อสาร (Free Speech) ที่ได้รับความคุ้มครองตามรัฐธรรมนูญฉบับแก้ไขเพิ่มเติมครั้งที่ 1²⁵ แนวทางของกฎหมายสหรัฐอเมริกานี้ ย่อมทำให้สามารถเสนอแนวทางในการปรับปรุงกฎหมายไทยให้มีความเหมาะสมมากยิ่งขึ้นได้

1.1 วัตถุประสงค์ของการวิจัย

1. เพื่อศึกษาแนวคิดและหลักกฎหมายที่มีความเกี่ยวข้องกับการหาตัวผู้กระทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ และการนำไปใช้ในการหาตัวผู้กระทำความผิดฐานหมิ่นประมาทโดยนิรนามในประเทศไทย

²¹ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 3 วรรคสี่.

²² พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 3 วรรคหก.

²³ Terry Hutchinson, ‘Doctrinal Research: Researching the Jury’ in Dawn Watkins and Mandy Burton (eds), *Research Methods in Law* (Routledge 2013) 9.

²⁴ รายละเอียดโปรดดูหัวข้อ 3.1.

²⁵ *McIntyre v Ohio Elections Commission*, 514 US 334 (1995).

2. เพื่อศึกษาเปรียบเทียบกระบวนการและแนวคิดของกฎหมายสหรัฐอเมริกาเกี่ยวกับกฎหมายไทย และนำเสนอกระบวนการที่กฎหมายไทยควรใช้เพื่อหาตัวผู้กระทำผิดฐานหมิ่นประมาทโดยนิรนาม

1.2 ขอบเขตของการวิจัย

การวิจัยครั้งนี้ ผู้วิจัยได้ศึกษาแนวคิดและหลักกฎหมายที่มีความเกี่ยวข้องกับการหาตัวผู้กระทำผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ พร้อมทั้งกรณีศึกษาที่เกี่ยวข้อง และวิเคราะห์ถึงการนำหลักกฎหมายนั้นไปใช้ในการหาตัวผู้กระทำผิดฐานหมิ่นประมาทในประเทศไทยว่า มีปัญหาอย่างไรบ้างและได้ศึกษากระบวนการและแนวคิดในการหาตัวผู้กระทำผิดฐานหมิ่นประมาทตามกฎหมายสหรัฐอเมริกาเพื่อนำมาใช้เป็นข้อเสนอในการพัฒนากฎหมายไทยให้สามารถหาตัวผู้กระทำผิดฐานหมิ่นประมาททางออนไลน์ได้อย่างมีประสิทธิภาพ

1.3 สมมติฐานการวิจัย

การสื่อสารออนไลน์เปิดโอกาสให้ผู้สื่อสารใช้นามแฝง (Pseudonym) หรือ ปิดบังตนเอง (Anonymous) ขณะสื่อสารก็ได้ หากบุคคลที่หมิ่นประมาทผู้อื่นใช้วิธีการเหล่านี้ขณะหมิ่นประมาทย่อมเป็นอุปสรรคต่อการดำเนินคดีทั้งทางอาญาและทางแพ่ง กฎหมายไทยได้แก้ไขปัญหานี้โดยการกำหนดกระบวนการไว้ใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ แต่กระบวนการนี้ยังมีปัญหาในทางปฏิบัติ จึงควรมีการปรับปรุงกระบวนการเพื่อให้ผู้เสียหายได้รับความคุ้มครองอย่างเหมาะสม

1.4 โจทย์การวิจัย

จากสมมติฐานข้างต้นโจทย์การวิจัย คือ ประเทศไทยควรกำหนดกระบวนการทางกฎหมายอย่างไรในการหาตัวผู้หมิ่นประมาทออนไลน์โดยนิรนาม

1.5 กรอบแนวคิดที่เกี่ยวข้องกับงานวิจัย

กรอบแนวคิดหลักที่ใช้ในการวิจัยครั้งนี้ คือ สิทธิในชื่อเสียง (Reputation) เป็นสิทธิที่ได้รับการคุ้มครองตามกฎหมายอาญาและแพ่งของไทย รวมถึงมีฐานะเป็นสิทธิตามรัฐธรรมนูญ แต่ในกรณีที่ผู้เสียหายถูกหมิ่นประมาททางออนไลน์โดยนิรนาม กฎหมายไทยยังไม่ได้คุ้มครองสิทธินี้อย่างเหมาะสม เพราะกระบวนการในการหาตัวผู้หมิ่นประมาทที่บัญญัติไว้ใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ยังไม่มีประสิทธิภาพเนื่องจากขึ้นอยู่กับความร่วมมือของหน่วยงานหลายหน่วยงานทั้งภาครัฐและเอกชน จึงควรมีการปรับปรุงกฎหมาย โดยกระบวนการที่ปรับปรุงนี้ต้องคำนึงถึงเสรีภาพในการสื่อสาร (Free Speech) ของผู้หมิ่นประมาทด้วย ทั้งนี้ ผู้วิจัยได้นำแนวทางของกฎหมายสหรัฐอเมริกา ซึ่งนำเสรีภาพในการสื่อสารมาใช้ประกอบการพิจารณาในกระบวนการเปิดเผยตัวผู้หมิ่นประมาทโดยนิรนาม มาเป็นแนวทางในการปรับปรุงกฎหมายไทย

ผู้วิจัยแบ่งเนื้อหาในบทความ ดังนี้ ในหัวข้อที่ 2 ผู้วิจัยจะนำเสนอกระบวนการหาตัวผู้กระทำผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ และวิเคราะห์ปัญหาที่เกิดขึ้นจากการใช้กระบวนการนี้กับความผิดฐานหมิ่นประมาท ในหัวข้อที่ 3 ผู้วิจัยจะนำเสนอกระบวนการที่กฎหมายสหรัฐอเมริกาใช้ในการหาตัวผู้หมิ่นประมาทโดยนิรนาม เพื่อเป็นแนวทางในการนำเสนอว่ากระบวนการในการหาตัวผู้หมิ่นประมาทที่เหมาะสมและสามารถป้องกันปัญหาที่เกิดขึ้นควรจะเป็นอย่างไรในหัวข้อที่ 4

2. กระบวนการทางกฎหมายในการหาตัวผู้กระทำผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ และการนำไปใช้กับคดีหมิ่นประมาท

ประเทศไทยได้กำหนดกระบวนการในการหาตัวผู้กระทำผิดทางอาญาที่เกี่ยวข้องกับคอมพิวเตอร์ โดยบัญญัติไว้ใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยการกำหนดให้ “พนักงานเจ้าหน้าที่” ซึ่งได้รับการแต่งตั้งตามมาตรา 28 ให้มีอำนาจตามมาตรา 18 ในการหาหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ อำนาจนี้รวมไปถึงอำนาจในการเรียกข้อมูลที่ “ผู้ให้บริการ” ต้องจัดเก็บตามมาตรา 26 กระบวนการนี้สามารถนำไปใช้ในการระบุตัวผู้กระทำผิดโดยหมิ่นประมาททางออนไลน์โดยนิรนามได้

พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้ให้นิยามคำว่า “ผู้ให้บริการ” ไว้ในมาตรา 3 วรรคสี่ ซึ่งแบ่งผู้ให้บริการออกเป็น 2 ประเภทใหญ่ ๆ ได้แก่

(1) ผู้ให้บริการแก่บุคคลอื่นในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่น โดยผ่านทางระบบคอมพิวเตอร์ ทั้งนี้ ไม่ว่าจะเป็นการให้บริการในนามของตนเอง หรือในนามหรือเพื่อประโยชน์ของบุคคลอื่น²⁶ เช่น ผู้ให้บริการกิจการโทรคมนาคมและกระจายภาพและเสียง (Telecommunication and Broadcast Carrier) ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ผู้ให้บริการร้านอินเทอร์เน็ตผู้ให้บริการสื่อสารสังคมออนไลน์²⁷

(2) ผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคลอื่น²⁸ เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอปพลิเคชันต่าง ๆ (Content and Application Service Provider)²⁹

พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้กำหนดให้ผู้ให้บริการข้างต้นมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (มาตรา 26 วรรคแรก) และเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ให้บริการนับแต่เริ่มใช้บริการ (มาตรา 26 วรรคสอง) (ดูหัวข้อ 2.1) ทั้งนี้ หากผู้ให้บริการที่ไม่ได้กระทำการตามที่กล่าวมานี้จะมีโทษทางอาญา (มาตรา 26 วรรคสี่) พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้ให้อำนาจพนักงานเจ้าหน้าที่เรียกข้อมูลที่ผู้ให้บริการมีหน้าที่จัดเก็บเพื่อใช้เป็นหลักฐานเกี่ยวกับการกระทำความผิด และหาตัวผู้กระทำความผิด (หัวข้อ 2.2) ทั้งนี้ ผู้วิจัยเห็นว่า กระบวนการนี้มีปัญหาในทางปฏิบัติเมื่อนำไปใช้กับการหาตัวผู้หมิ่นประมาทโดยนิรนาม (หัวข้อ 2.3)

2.1 หน้าที่ของผู้ให้บริการในการเก็บรักษาข้อมูล

พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ มาตรา 26 วรรคหนึ่ง ได้กำหนดให้ผู้ให้บริการมีหน้าที่เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ ทั้งนี้ มาตรา 3 วรรคสาม ได้ให้ความหมายของ “ข้อมูลจราจรทางคอมพิวเตอร์” ดังนี้

²⁶ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 3 วรรคสี่ (1).

²⁷ ตัวอย่างของผู้ให้บริการประเภทที่ (1) นำมาจากประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ข้อ 5(1).

²⁸ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 3 วรรคสี่ (2).

²⁹ ตัวอย่างของผู้ให้บริการประเภทที่ (2) นำมาจากประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2564 ข้อ 5(2).

ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

คุณสรุเชษฐ์ ขาติชาคร ได้อธิบายรายละเอียดว่า ข้อมูลจราจรทางคอมพิวเตอร์ “แสดงให้เห็นถึงระบบคอมพิวเตอร์ที่ส่งข้อมูล และรับข้อมูลของการติดต่อสื่อสารนั้น ช่วงเวลาและระยะเวลาที่มีการติดต่อสื่อสาร ลักษณะของข้อมูลที่รับส่ง และเส้นทางที่ใช้ในการส่งข้อมูลดังกล่าว หรือ อาจกล่าวได้ว่า ข้อมูลจราจรทางคอมพิวเตอร์เป็นร่องรอยที่เกิดขึ้นเมื่อมีการติดต่อสื่อสารของระบบคอมพิวเตอร์”³⁰ คำอธิบายนี้ทำให้เห็นว่า ข้อมูลจราจรทางคอมพิวเตอร์แสดงให้เห็น “ร่องรอยการติดต่อสื่อสาร” แต่ไม่ได้แสดงว่าใครเป็นคนสื่อสาร ดังนั้น มาตรา 26 วรรคสอง จึงกำหนดให้ผู้ให้บริการเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็น ในการระบุตัวผู้ให้บริการ ดร.สุนติ คงเทพ ได้อธิบายว่า ในทางปฏิบัติผู้ให้บริการจะต้องมีกระบวนการพิสูจน์ตัวตนก่อนที่จะให้ผู้ให้บริการเข้าไปใช้บริการ กระบวนการนี้กำหนดให้ผู้ให้บริการกรอกชื่อผู้ให้บริการ หมายเลขบัตรประชาชน หรือ หมายเลขหนังสือเดินทางก่อนที่จะเข้าไปใช้บริการ³¹ พนักงานเจ้าหน้าที่ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ มีอำนาจตามมาตรา 18 วรรคหนึ่ง (2) และ (3)³² ในการเรียกข้อมูลที่กำลังกล่าวมานี้เพื่อประโยชน์ในการสืบสวนและสอบสวนการกระทำความผิดตามกฎหมายนี้ได้ แต่ในกรณีการสืบสวนหรือสอบสวนความผิดตามกฎหมายอื่นที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด (เช่น การหมิ่นประมาท) พนักงานสอบสวนตามกฎหมายอื่นต้องขอข้อมูลข้างต้นจากพนักงานเจ้าหน้าที่ ฯ ซึ่งจะได้อธิบายโดยละเอียดในหัวข้อต่อไป

2.2 กระบวนการหาตัวผู้กระทำความผิดซึ่งใช้สื่อออนไลน์เป็นเครื่องมือ และกรณีศึกษา

2.2.1 การหาตัวผู้กระทำความผิดซึ่งใช้สื่อออนไลน์เป็นเครื่องมือตามมาตรา 18

พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้กำหนดให้มี “พนักงานเจ้าหน้าที่” ซึ่งแต่งตั้งโดยรัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเป็นบุคคลที่มีอำนาจในการสืบสวนและสอบสวนการกระทำความผิดตามกฎหมายฉบับนี้³³ ในกรณีที่เป็นการกระทำความผิดอาญาฐานอื่นที่มีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด ผู้เสียหายต้องดำเนินการตามประมวลกฎหมายวิธีพิจารณาความอาญา กล่าวคือ ต้องร้องทุกข์ต่อพนักงานสอบสวนตามกฎหมายวิธีพิจารณาความอาญา ทั้งนี้ ศาสตราจารย์ ดร.สรารุช ปิตียาศักดิ์ ได้อธิบายเพิ่มเติมว่า พนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ยังคงมีอำนาจดำเนินคดีที่เกี่ยวกับการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ เพียงแต่พนักงานสอบสวนจะไม่สามารถใช้อำนาจที่กำหนดไว้ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ได้³⁴ กล่าวคือ พนักงานสอบสวนมีอำนาจสอบสวนการทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ แต่พนักงานสอบสวนไม่มีอำนาจที่กำหนดไว้ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ เช่น อำนาจตามมาตรา 18 วรรคหนึ่ง ในการเรียก

³⁰ สรุเชษฐ์ ขาติชาคร, ‘ปัญหาการจัดเก็บและการได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์เพื่อนำไปใช้เป็นพยานหลักฐานในคดีละเมิดลิขสิทธิ์ทางอินเทอร์เน็ต’ (วิทยานิพนธ์ นิติศาสตรมหาบัณฑิต มหาวิทยาลัยกรุงเทพ 2557) 38.

³¹ สุนติ คงเทพ, *กฎหมายเกี่ยวกับคอมพิวเตอร์* (พิมพ์ครั้งที่ 2 มังกรูต ดิจิตอลเพรส 2561) 443.

³² พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 18 วรรคหนึ่ง (2) และ (3).

³³ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 29 วรรคแรก.

³⁴ สรารุช ปิตียาศักดิ์, *คำอธิบาย พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560* (พิมพ์ครั้งที่ 3 นิติธรรม 2565) 253.

ข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการเกี่ยวกับการติดต่อสื่อสารผ่านระบบคอมพิวเตอร์หรือจากบุคคลอื่นที่เกี่ยวข้อง (ตามมาตรา 18 วรรคหนึ่ง (2)) กรณีเช่นนี้ พนักงานสอบสวนต้องร้องขอให้พนักงานเจ้าหน้าที่ ใช้อำนาจตามมาตรา 18 วรรคหนึ่ง เพื่อหาตัวผู้กระทำความผิด

อำนาจของพนักงานเจ้าหน้าที่ ๓ ที่ระบุในมาตรา 18 วรรคหนึ่ง เป็นอำนาจในการสืบสวนและสอบสวนเพื่อหาหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๓ อำนาจนี้รวมไปถึง³⁵

- อำนาจในการเรียกข้อมูลจราจรทางคอมพิวเตอร์จากผู้ให้บริการตามมาตรา 18 วรรคหนึ่ง (2) ที่ได้กล่าวไปแล้วข้างต้น

- อำนาจในการสั่งให้ผู้ให้บริการส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 หรือที่อยู่ในความครอบครองหรือควบคุมของผู้ให้บริการ ให้แก่พนักงานเจ้าหน้าที่หรือให้เก็บข้อมูลดังกล่าวไว้ก่อน ตามมาตรา 18 วรรคหนึ่ง (3)

- อำนาจในการทำสำเนาข้อมูลคอมพิวเตอร์ ข้อมูลจราจรทางคอมพิวเตอร์จากระบบคอมพิวเตอร์ที่มีเหตุอันควรเชื่อได้ว่าการกระทำความผิด ในกรณีที่ระบบคอมพิวเตอร์นั้นยังมิได้อยู่ในความครอบครองของพนักงานเจ้าหน้าที่ ตามมาตรา 18 วรรคหนึ่ง (4)

ในกรณีที่พนักงานเจ้าหน้าที่ ๓ ต้องการทำสำเนาข้อมูลข้างต้น พนักงานเจ้าหน้าที่ต้องยื่นคำร้องต่อศาลที่มีเขตอำนาจ เพื่อให้ศาลมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง³⁶

อำนาจที่กล่าวมานี้เป็นอำนาจของพนักงานเจ้าหน้าที่ ๓ ที่ระบุไว้ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๓ เพื่อสืบสวนและสอบสวนการกระทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๓ หากมีการกระทำความผิดอาญาฐานอื่นโดยใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด เช่น การหมิ่นประมาททางออนไลน์ พนักงานสอบสวนของความผิดฐานนั้นต้องร้องขอตามมาตรา 18 วรรคสอง ให้พนักงานเจ้าหน้าที่ ๓ ใช้อำนาจตามมาตรา 18 วรรคหนึ่งเพื่อหาหลักฐานเกี่ยวกับการกระทำความผิดและหาตัวผู้กระทำความผิด³⁷

2.2.2 กรณีศึกษา

ผู้วิจัยพบว่า มีงานวิจัยของ Ghazi-Tehrani ที่ได้มีการกล่าวถึงการดำเนินคดีกับผู้กระทำความผิดทางออนไลน์ที่ไม่ได้เปิดเผยตัวตนซึ่งต้องมีการหาหลักฐานจากคอมพิวเตอร์เพื่อใช้ในการหาตัวผู้กระทำ เช่น ในคดีสื่อลามกอนาจารเด็ก (Child Pornography)³⁸ Ghazi-Tehrani ได้เล่าว่า ในช่วงปี 2556 ตำรวจสากลได้ติดต่อไปยังกองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีของสำนักงานตำรวจแห่งชาติว่า มีเว็บไซต์ซึ่งมีภาพลามกอนาจารเด็กในประเทศไทย ทางกองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีตรวจสอบไปที่ WHOIS แล้วพบข้อมูลต่อไปนี้ (1) เบอร์โทรผู้กระทำความผิดซึ่งเป็นเลขหมายเติมเงินซึ่งไม่สามารถตามต่อได้ (2) อีเมลของผู้กระทำความผิดซึ่งเป็น Gmail ที่ไม่สามารถติดตามต่อได้เช่นกัน และ (3) เว็บไซต์ให้บริการโฮสติ้ง (Hosting Service) ของบริษัทในฮ่องกง

³⁵ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 18 วรรคหนึ่ง.

³⁶ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 19 วรรคหนึ่ง.

³⁷ พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 มาตรา 18 วรรคสอง.

³⁸ Adam Ghazi-Tehrani, 'The Current State of Cybercrime in Thailand: Legal Technological and Economic Barriers to Effective Law Enforcement' (2015) 1(2) Social Science Asia 1, 10-12.

อย่างไรก็ตาม แม้ Gmail จะไม่สามารถตามไปถึงตัวบุคคลได้ แต่ทางตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีได้พบว่ามีผู้ใช้อีเมลนี้ในเว็บบอร์ด (Web Board) แห่งหนึ่ง และผู้ใช้คนนี้ให้อีเมลอีกอันหนึ่งซึ่งเป็นอีเมลของนักเรียนในโรงเรียนแห่งหนึ่ง ทางตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยีจึงได้ขอข้อมูลของผู้ใช้อีเมลจากโรงเรียนแห่งนั้นทำให้พบว่า เจ้าของอีเมลนี้เป็นนักเรียนของโรงเรียนนี้ และสามารถติดต่อนักเรียนคนนี้เพื่อให้ทำการปิดเว็บไซต์ได้ อย่างไรก็ตาม ไม่ได้มีการดำเนินคดีนักเรียนคนนี้แต่อย่างใด

นอกจากนี้ ในงานวิจัยของ Ghazi-Tehrani ยังได้กล่าวถึง **คดี Twitter Hack** ซึ่งเป็นเรื่องที่ Twitter ของ นายกรัฐมนตรีในขณะนั้นถูกแฮกเมื่อเดือนตุลาคม พ.ศ. 2554³⁹ Ghazi-Tehrani ได้เล่าว่า แฮกเกอร์ (Hacker) เป็นนักศึกษามหาวิทยาลัยแห่งหนึ่งซึ่งไม่ได้พยายามที่จะขโมย IP Address ขณะที่ตนเองได้เข้าถึง Twitter ของนายกรัฐมนตรีท่านนี้ กรณีนี้ Twitter และผู้ให้บริการอินเทอร์เน็ตของแฮกเกอร์ได้ให้ความร่วมมือกับหน่วยงานของรัฐในการให้ข้อมูลเพื่อตามหาแฮกเกอร์คนนี้ แฮกเกอร์จึงถูกจับในเวลาไม่ช้าและถูกแจ้งข้อหาความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ แต่ก็ได้มีการฟ้องศาลแต่อย่างใด⁴⁰

ในงานวิจัยของ Ghazi-Tehrani ไม่ได้ให้รายละเอียดว่า โรงเรียนในคดีสื่อลามกอนาจารเด็ก ได้ให้ข้อมูลอะไรกับกองบังคับการตำรวจสืบสวนสอบสวนอาชญากรรมทางเทคโนโลยี ผู้วิจัยเห็นว่า โรงเรียนมีฐานะเป็น “ผู้ให้บริการ” ที่ต้องเก็บข้อมูลเกี่ยวกับผู้ใช้บริการตามมาตรา 26 เพื่อระบุว่า อีเมลใดเป็นของนักเรียนคนไหน เจ้าหน้าที่ตำรวจจึงมีข้อมูลยืนยันว่า นักเรียนคนนี้เป็นเจ้าของอีเมลที่เชื่อมโยงไปยัง Gmail ของเจ้าของเว็บไซต์นี้ และ Ghazi-Tehrani ไม่ได้ลงรายละเอียดเช่นกันว่า ในคดี Twitter Hack ทาง Twitter และผู้ให้บริการอินเทอร์เน็ตได้ให้ข้อมูลอะไรบ้าง ผู้วิจัยเห็นว่า กรณีนี้ Twitter และผู้ให้บริการอินเทอร์เน็ตมีหน้าที่ในการให้ข้อมูลของผู้ใช้บริการซึ่งต้องจัดเก็บตามมาตรา 26 เช่นกัน ตัวอย่างทั้งสองเรื่องนี้ทำให้ผู้วิจัยเห็นว่า ข้อมูลที่ผู้ให้บริการต้องจัดเก็บเป็นเครื่องมือสำคัญในการดำเนินคดี และหาตัวผู้กระทำความผิดทางออนไลน์โดยนิรนามได้

นอกจากตัวอย่างข้างต้นแล้ว ผู้วิจัยได้พบว่า มีคดีที่ศาลใช้ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการต้องจัดเก็บเป็นหลักฐานสำคัญเพื่อระบุว่าจำเลยเป็นผู้กระทำความผิดจริง คือ **คำพิพากษาศาลฎีกาที่ 3473/2563** คดีนี้เป็นความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ศาลวินิจฉัยว่า จำเลยกระทำความผิดตามมาตรา 5 โดยศาลรับฟังข้อเท็จจริงโดยปราศจากเหตุอันควรสงสัยว่า จำเลยได้ใช้เครื่องคอมพิวเตอร์จากภายนอกผ่านระบบอินเทอร์เน็ตของผู้ให้บริการอินเทอร์เน็ต เข้าสู่เครื่องคอมพิวเตอร์แม่ข่ายของโรงพยาบาล ฯ แล้วทำการปิดระบบกระจายสัญญาณเพื่อปิดระบบโปรแกรมสำหรับบริการทางการแพทย์

สำหรับข้อเท็จจริงที่ทำให้ศาลฎีกาเห็นว่า “จำเลยเป็นผู้กระทำความผิดโดยปราศจากเหตุอันควรสงสัย” คือ การเข้าสู่ระบบเครือข่ายคอมพิวเตอร์ของโรงพยาบาล ฯ ผู้เข้าสู่ระบบจะต้องทราบชื่อผู้ใช้และรหัสผ่านจึงจะสามารถเข้าสู่ระบบได้ เมื่อข้อเท็จจริงฟังได้ว่า

- (1) จำเลยเป็นหนึ่งในหกคนเท่านั้นที่ทราบชื่อผู้ใช้และรหัสผ่าน เพราะจำเลยเป็นผู้วางระบบ

³⁹ ibid 11-12.

⁴⁰ นอกจากทั้งสองคดีนี้แล้ว Ghazi-Tehrani ยังได้กล่าวถึงการดำเนินการเพื่อหาตัวผู้กระทำความผิดอีก 1 คดี Cyber Extortion ผู้สนใจสามารถเข้าไปอ่านได้ที่ ibid 12-13.

(2) เมื่อตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ย้อนหลังไปในเวลาเกิดเหตุปรากฏว่า มีการใช้หมายเลข IP: 223.207.16x.xxx และหมายเลข IP: 223.205.10x.xxx ในช่วงเวลาเกิดเหตุซึ่งเป็น IP Address ของบริษัทที่มีจำเลยเป็นกรรมการ โจทก์มีพนักงานสอบสวนผู้ขอข้อมูลจากผู้ให้บริการมาเบิกความประกอบข้อมูลจราจรทางคอมพิวเตอร์ยืนยันว่า ผู้ให้บริการอินเทอร์เน็ตตรวจสอบหมายเลข IP ดังกล่าวว่าเป็นผู้ใช้บริการ และมีหนังสือแจ้งผลการตรวจสอบมา ไม่ปรากฏข้อสงสัยว่า ผู้ให้บริการจะกลั่นแกล้งให้ร้ายจำเลย หรือมีข้อพิรุธแต่ประการใด

นอกจากนี้ศาลได้อธิบายว่า เมื่อจำเลยเป็นผู้วางระบบคอมพิวเตอร์ และติดตั้งเครือข่ายคอมพิวเตอร์ให้โรงพยาบาล ฯ หากระบบดังกล่าวขัดข้อง ย่อมเป็นธรรมดาที่โรงพยาบาล ฯ จะแก้ไขปรับปรุงเพื่อให้สามารถใช้งานได้อย่างมีประสิทธิภาพ จำเลยอยู่ในข่ายที่จะได้รับประโยชน์หากได้รับมอบหมายให้ดำเนินการ ดังนั้น แม้โจทก์ไม่มีประจักษ์พยานรู้เห็นเหตุการณ์ขณะจำเลยใช้เครื่องคอมพิวเตอร์จากภายนอกผ่านระบบอินเทอร์เน็ตเข้าสู่เครื่องคอมพิวเตอร์ของโรงพยาบาล ฯ หรือไม่มีการตรวจยึดเครื่องคอมพิวเตอร์เครื่องใด ชนิดใดจากจำเลยไปตรวจสอบก็ไม่ทำให้พยานหลักฐานของโจทก์มีน้ำหนักลดน้อยลงจนถึงกับรับฟังไม่ได้

คำพิพากษานี้แสดงให้เห็นว่า ข้อมูลจราจรทางคอมพิวเตอร์ที่ผู้ให้บริการมีหน้าที่จัดเก็บ เป็นหลักฐานที่สำคัญที่ใช้เพื่อหาตัวผู้กระทำความผิดตามกฎหมาย ทั้งนี้ ความผิดตามคำพิพากษานี้ และความผิดของสองคดีที่ได้กล่าวไปข้างต้น เป็นความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยตรง ซึ่งพนักงานเจ้าหน้าที่ ฯ ตามกฎหมายนี้สามารถใช้อำนาจตามมาตรา 18 วรรคหนึ่ง (2) และ (3) เพื่อขอข้อมูลได้โดยตรง

กรณีที่มีการทำความผิดอื่นที่ไม่ใช่การทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ แต่ผู้กระทำได้ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิด พนักงานสอบสวนคดีความผิดเหล่านี้ต้องขอให้พนักงานเจ้าหน้าที่ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ดำเนินการเพื่อขอข้อมูลจากผู้ให้บริการประเด็นนี้ คุณสุรเชษฐ์ ฯ ได้อธิบายถึงการใช้กระบวนการนี้ในการหาตัวผู้กระทำความผิดฐานละเมิดลิขสิทธิ์ทางอินเทอร์เน็ต ซึ่งเป็นความผิดอาญาที่ไม่ใช่ความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ โดยได้สัมภาษณ์พนักงานสอบสวนซึ่งได้รับแต่งตั้งให้เป็นพนักงานเจ้าหน้าที่ ฯ และสัมภาษณ์พนักงานของผู้ให้บริการเพื่อสอบถามถึงกระบวนการขอข้อมูลเพื่อหาตัวผู้กระทำความผิด⁴¹ เมื่อนำกระบวนการนี้มาใช้กับการหาตัวผู้หมิ่นประมาท จะสามารถสรุปได้ ดังนี้

- (1) พนักงานสอบสวนของคดีหมิ่นประมาทออนไลน์ส่งหนังสือร้องขอให้พนักงานเจ้าหน้าที่ ฯ
- (2) พนักงานเจ้าหน้าที่ ฯ ติดต่อไปยังผู้ให้บริการที่เกี่ยวข้องกับการหมิ่นประมาทออนไลน์
- (3) พนักงานของผู้ให้บริการตรวจสอบว่า การให้บริการของตนมีความเกี่ยวข้องกับผู้กระทำความผิดหรือไม่ และตรวจสอบว่ามีข้อมูลที่ขอมาหรือไม่
- (4) ในกรณีที่ผู้ให้บริการมีข้อมูลที่เกี่ยวข้อง ผู้ให้บริการจะส่งข้อมูลนั้นไปยังพนักงานเจ้าหน้าที่ ฯ
- (5) พนักงานเจ้าหน้าที่ ฯ ส่งข้อมูลนั้นต่อไปยังพนักงานสอบสวนคดีหมิ่นประมาท เพื่อดำเนินคดีหมิ่นประมาทตามกระบวนการของกฎหมายวิธีพิจารณาความอาญา

กระบวนการข้างต้นทำให้เห็นว่า โจทก์ในคดีหมิ่นประมาทสามารถดำเนินการเพื่อให้ได้มาซึ่งข้อมูลจราจรทางคอมพิวเตอร์ และข้อมูลของผู้ใช้บริการเพื่อใช้ในการระบุตัวผู้หมิ่นประมาททางออนไลน์โดยนิตินามได้ และเมื่อโจทก์นำข้อมูลเหล่านี้มาแสดงต่อศาล ศาลย่อมรับฟังโดยปราศจากเหตุอันควรสงสัยว่า จำเลย คือ

⁴¹ สุรเชษฐ์ ขาดิชาคร (n 30) 50.

คนหมิ่นประมาท ทำให้ศาลลงโทษ ให้จำเลยรับผิดชอบหมิ่นประมาทเหมือนกับการลงโทษจำเลยใน คำพิพากษาฎีกาที่ 3473/2563

ในทางตรงกันข้าม ผู้วิจัยได้พบว่ามีคำพิพากษาฎีกาที่ศาลยกฟ้องโจทก์ เพราะโจทก์ไม่ได้นำสืบข้อมูล จราจรทางคอมพิวเตอร์เพื่อให้ศาลเชื่อว่า จำเลยเป็นผู้ส่งจดหมายอิเล็กทรอนิกส์ที่มีเนื้อหาหมิ่นประมาท คือ คำพิพากษาฎีกาที่ 952/2563 ในคดีนี้ โจทก์ฟ้องว่าจำเลยได้ส่งจดหมายอิเล็กทรอนิกส์ที่มีข้อความหมิ่น ประมาทโจทก์ร่วม โดยในจดหมายนี้มีชื่อและที่อยู่ของผู้ส่ง คือ จำเลยที่ 1 แต่มีแถบสีดำปิดบังข้อมูลสำคัญอัน เป็นพิรุณต่างจากจดหมายอิเล็กทรอนิกส์โดยทั่วไป และจำเลยที่ 1 ปฏิเสธมาตั้งแต่ต้นว่า มิได้เป็นผู้ส่งจดหมาย อิเล็กทรอนิกส์ทั้งสองฉบับ ทั้งนี้ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๖ มาตรา 26 วรรคหนึ่ง ให้ผู้ให้บริการ ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ เพื่อประโยชน์ในการตรวจสอบการส่งข้อมูลการสื่อสารทาง คอมพิวเตอร์ แต่โจทก์ไม่ได้นำสืบถึงข้อมูลจราจรทางคอมพิวเตอร์ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงให้เห็น จำเลยที่ 1 เป็นผู้ส่ง นอกเหนือไปจากการที่เอกสารดังกล่าวมีชื่อและที่อยู่ของจำเลยที่ 1 ซึ่งสามารถปลอม แปลงโดยผู้อื่นได้

แม้การที่จำเลยที่ 1 มีข้อขัดแย้งกับโจทก์ร่วมมาก่อน ไม่อาจเป็นข้อสนับสนุนว่าจำเลยที่ 1 เป็นผู้ส่ง จดหมายอิเล็กทรอนิกส์ได้ เพราะได้ความตามทางนำสืบของโจทก์และโจทก์ร่วมเองว่า โจทก์ร่วมมีข้อขัดแย้ง กับคนอื่นอีกหลายรายอันอาจสร้างความไม่พอใจแก่บุคคลเหล่านั้น นอกจากนี้ ยังมีบุคคลซึ่งไม่ทราบว่าเป็น ผู้ใดจัดทำใบปลิวมีข้อความโจมตีกล่าวหาโจทก์ร่วมนำไปปิดและวางเผยแพร่ตามสถานที่สาธารณะ โจทก์และ โจทก์ร่วมไม่มีพยานหลักฐานใดมานำสืบสนับสนุนให้ฟังได้ว่า จำเลยที่ 1 เป็นผู้จัดทำหรือเผยแพร่ใบปลิว ดังกล่าว ดังนั้น รูปคดีนี้บ่งชี้ว่ายังมีเหตุสงสัยตามสมควรว่าจำเลยที่ 1 ส่งจดหมายอิเล็กทรอนิกส์ไปยังบุคคลต่าง ๆ หรือไม่ จึงให้ยกประโยชน์แห่งความสงสัยนั้นให้จำเลยที่ 1 ตามประมวลกฎหมายวิธีพิจารณาความอาญา มาตรา 227 วรรคสอง จำเลยที่ 1 จึงไม่มีความผิด

คดีนี้ ทำให้เห็นว่าเมื่อโจทก์ไม่สามารถพิสูจน์ได้ว่า จำเลยเป็นผู้ส่งข้อความหมิ่นประมาทจริง ๆ เพราะโจทก์ไม่ได้แสดงรายละเอียดข้อมูลจราจรทางคอมพิวเตอร์ของจดหมายอิเล็กทรอนิกส์ที่ผู้ให้บริการมี หน้าที่จัดเก็บเพื่อยืนยันว่าจำเลยเป็นคนส่ง แม้โจทก์ร่วมและจำเลยที่ 1 มีปัญหากัน แต่เมื่อโจทก์ร่วมมีปัญหา กับคนอื่น ๆ ด้วย จึงยังเป็นที่สงสัยว่า จำเลยส่งจดหมายอิเล็กทรอนิกส์ที่มีข้อความหมิ่นประมาทจริงหรือไม่ ศาลจึงยกฟ้องจำเลย

จากหลักกฎหมายและกรณีศึกษาข้างต้นทำให้เห็นว่า ข้อมูลที่ผู้ให้บริการมีหน้าที่ในการจัดเก็บตาม มาตรา 26 มีความสำคัญมากในการดำเนินคดีในกรณีที่ไม่สามารถระบุตัวผู้กระทำผิดได้อย่างชัดเจน

2.3 ปัญหาของกระบวนการหาตัวผู้กระทำผิด

จากเนื้อหาที่นำเสนอข้างต้นแสดงให้เห็นถึงกระบวนการหาตัวผู้กระทำผิดที่กำหนดไว้ใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๖ พร้อมทั้งกรณีศึกษาที่แสดงให้เห็นผลของการนำกระบวนการนั้นไปใช้ แต่ผู้วิจัยเห็นว่ากระบวนการนี้มีความซับซ้อนเพราะขึ้นอยู่กับความร่วมมือของหน่วยงานภาครัฐและเอกชน หากมีฝ่ายใดปฏิเสธที่จะให้ความร่วมมือ กระบวนการนี้ย่อมไม่สามารถหาตัวผู้กระทำผิดได้ ผู้วิจัยพบว่า มีงาน วิชาการที่ศึกษาเกี่ยวกับปัญหาการบังคับใช้ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๖ ซึ่งแสดงให้เห็นว่า กระบวนการนี้มีปัญหาทางปฏิบัติในการหาตัวผู้กระทำผิดสรุปได้ 2 ประการ และยังมีการตั้งคำถามว่า การหา ตัวผู้กระทำผิดถือเป็นการละเมิดสิทธิความเป็นอยู่ส่วนตัวเกินสมควรหรือไม่

ปัญหาประการแรก ศาสตราจารย์ ดร. สุธรรม เชื้อประกอบกิจ และ รองศาสตราจารย์ ดร.กิตติธนัท เลอวงศ์รัตน์⁴² ได้นำเสนอว่าอุปสรรคประการหนึ่งในการจัดการความผิดเกี่ยวกับคอมพิวเตอร์ คือ ผู้ให้บริการอินเทอร์เน็ตปฏิเสธที่จะให้ความร่วมมือกับพนักงานสอบสวน ในการส่งข้อมูลคอมพิวเตอร์ และข้อมูลจราจรทางคอมพิวเตอร์ ผู้วิจัยทั้งสองท่านนี้เห็นว่า การไม่มีข้อมูลเหล่านี้ทำให้โอกาสในการระบุตัวผู้กระทำความผิดมีน้อย ซึ่งสอดคล้องกับมุมมองของผู้วิจัยที่ว่า ความร่วมมือระหว่างพนักงานเจ้าหน้าที่และผู้ให้บริการมีความสำคัญเป็นอย่างมากในการหาตัวผู้กระทำความผิด

นอกจากนี้ คุณอิสรพงศ์ ทิพย์อากาศ และคณะ⁴³ ซึ่งได้ทำการศึกษาเกี่ยวกับการสืบสวนคดีการฉ้อโกงออนไลน์⁴⁴ ซึ่งเป็นความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๒ เช่นกัน ได้กล่าวว่า “การร้องขอข้อมูลจากผู้ให้บริการเป็นปัญหาเป็นอย่างมาก⁴⁵” ผู้ให้บริการมักปฏิเสธที่จะให้ความร่วมมือ หากคำขออนุญาตไม่ได้มาจากพนักงานเจ้าหน้าที่ ๒ ทางคุณอิสรพงศ์และคณะ ๒ มีความเห็นว่า พนักงานสอบสวนควรจะมีอำนาจขอข้อมูลนั้นได้ อย่างไรก็ตาม ผู้วิจัยพบว่า คณะกรรมการกฤษฎีกาเคยมีความเห็นในประเด็นเรื่องอำนาจของพนักงานสอบสวนในการขอข้อมูลจากผู้ให้บริการ เพื่อหาตัวผู้กระทำความผิดที่ใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำความผิดใน **ความเห็นทางกฎหมายที่ 343/2549** (ก่อนมีการบัญญัติ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๒) ความเห็นนี้ได้อธิบายว่า เพื่อประโยชน์ในการระบุตัวบุคคลที่จัดทำเว็บไซต์ที่ไม่ชอบด้วยกฎหมาย หรือ กระทำความผิดอาญาฐานอื่น พนักงานสอบสวนมีอำนาจเรียกให้ผู้ให้บริการส่งข้อมูลดังต่อไปนี้ได้ คือ ชื่อผู้ให้บริการ ที่อยู่และเบอร์โทรศัพท์ที่ใช้ในการเชื่อมต่ออินเทอร์เน็ต รวมไปถึงระยะเวลาที่ผู้ให้บริการได้เข้าไปสู่ระบบคอมพิวเตอร์เพื่อทำผิดกฎหมาย ทั้งนี้ พนักงานสอบสวนสามารถเรียกข้อมูลนี้ได้โดยไม่ต้องขออนุญาตจากศาล⁴⁵

หากนำข้อมูลที่พนักงานสอบสวนมีอำนาจเรียกตาม **ความเห็นทางกฎหมายที่ 343/2549** มาเปรียบเทียบกับข้อมูลที่ผู้ให้บริการจะต้องจัดเก็บตามมาตรา 26 จะเห็นว่า ข้อมูลเหล่านี้ คือ ข้อมูลที่ผู้ให้บริการต้องเก็บรักษาไว้ตามมาตรา 26 วรรคสอง ซึ่งพนักงานเจ้าหน้าที่ ๒ มีอำนาจเรียกได้ตามมาตรา 18 วรรคหนึ่ง (2) แต่ข้อมูลที่กล่าวมานี้ไม่ครอบคลุมถึงข้อมูลจราจรคอมพิวเตอร์ทุกประเภทตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๒ ซึ่งเป็นกฎหมายที่บัญญัติขึ้นภายหลังและมีความละเอียดกว่า ดังนี้ จึงเกิดปัญหาในการตีความกฎหมายว่า (ก) พนักงานสอบสวนมีอำนาจเรียกข้อมูลจราจรคอมพิวเตอร์ที่อยู่ข้อบัญญัติใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๒ หรือไม่ หรือ (ข) อำนาจที่พนักงานสอบสวนเคยมีตาม **ความเห็นทางกฎหมายที่ 343/2549** จะกลายเป็นอำนาจของพนักงานเจ้าหน้าที่ ๒ ภายหลัง พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๒

⁴² Sutham Cheurprakobkit and Kidtanathat Lerwongrat, ‘Criminal Justice Officials’ Attitudes towards Addressing Computer Crimes in Thailand: Difficulties and Recommendations’ (2025) 28 Trends Organized Crime 293.

⁴³ Essarapong Tiprapakool and others, ‘Model of Cyber Crime Investigation in Thailand: Fraudulent Cases’ (2021) 12(6) Turkish Online Journal of Qualitative Inquiry 9365.

⁴⁴ ibid 9367.

⁴⁵ ‘บันทึกสำนักงานคณะกรรมการกฤษฎีกา เรื่อง อำนาจของเจ้าพนักงานตำรวจในการปิดกั้นเว็บไซต์ที่ไม่เหมาะสมทางอินเทอร์เน็ต และของพนักงานสอบสวนตามมาตรา 132’ (คณะกรรมการพัฒนากฎหมาย สำนักงานคณะกรรมการกฤษฎีกา, 2549) <<https://www.lawreform.go.th/uploads/files/news424.pdf>> สืบค้นวันที่ 11 สิงหาคม 2568.

มีผลบังคับใช้แล้ว ดังนั้น ผู้ให้บริการจึงไม่มีความมั่นใจที่จะส่งข้อมูลไปให้กับเจ้าหน้าที่ของรัฐที่ไม่ใช่พนักงานเจ้าหน้าที่ ๖

งานวิจัยที่ระบุถึงปัญหาข้างต้นเป็นงานวิจัยที่เกี่ยวข้องกับการกระทำความผิดตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๖ โดยตรง แต่กลับพบว่า ผู้ให้บริการปฏิเสธในการให้ความร่วมมือกับพนักงานเจ้าหน้าที่ ทำให้ผู้วิจัยเห็นว่า ความไม่ชัดเจนของกฎหมายเช่นนี้ย่อมทำให้พนักงานสอบสวนที่ทำคดีหมิ่นประมาทไม่ได้รับความร่วมมือจากผู้ให้บริการในการให้ข้อมูลเพื่อหาตัวผู้หมิ่นประมาทโดยนิรนามเช่นกัน

ปัญหาประการที่สอง จำนวนบุคลากรที่ต้องใช้อำนาจในการดำเนินคดีเป็นอุปสรรคอีกประการหนึ่ง โดยในงานวิจัยของ Ghazi-Tehrani และของคุณอิสพรพงศ์ ๖ และคณะ ๖ มีความเห็นในทางเดียวกันว่า จำนวนพนักงานเจ้าหน้าที่ซึ่งทำหน้าที่ในการดำเนินคดีมีจำนวนน้อย หากเทียบกับการใช้อินเทอร์เน็ตในประเทศไทย⁴⁶ งานวิจัยที่กล่าวมานี้เป็นงานวิจัยเกี่ยวกับ พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ๖ โดยตรงแต่กลับพบว่า จำนวนบุคลากรที่ต้องบังคับใช้กฎหมายฉบับนี้ยังไม่เพียงพอ ผู้วิจัยจึงเห็นว่าจำนวนพนักงานเจ้าหน้าที่ ๖ ซึ่งจะต้องช่วยพนักงานสอบสวนหาผู้กระทำความผิดตามกฎหมายอื่น (เช่น ความผิดฐานหมิ่นประมาท) ย่อมไม่เพียงพอต่อการกระทำผิดที่เกิดขึ้น ทั้งนี้ ตามที่ปรากฏในคำพิพากษาศาลฎีกาที่ 952/2563 การที่โจทก์ไม่ได้นำสืบให้ปรากฏถึงรายละเอียดข้อมูลจราจรทางคอมพิวเตอร์ในคดีหมิ่นประมาทเป็นเหตุให้ศาลยกฟ้องได้

นอกจากปัญหาข้างต้นแล้ว องค์กร Article19⁴⁷ ได้ตั้งคำถามว่า กระบวนการในการหาตัวผู้กระทำความผิดเป็นการละเมิดสิทธิความเป็นอยู่ส่วนตัวของบุคคลเกินสมควรหรือไม่ องค์กรนี้ให้ความเห็นว่า⁴⁸ กระบวนการตามมาตรา 18 วรรคหนึ่ง (1) - (3) ซึ่งให้อำนาจพนักงานเจ้าหน้าที่ ๖ ใช้ได้โดยไม่ต้องขออนุญาตศาลไม่ได้คำนึงถึงการรับรองสิทธิในความเป็นอยู่ส่วนตัว (Right to Privacy) องค์กรนี้เห็นว่าบทบัญญัตินี้ไม่ได้กำหนดให้ศาลทำการตรวจสอบ แต่ให้เจ้าหน้าที่บังคับให้ผู้ให้บริการเปิดเผยข้อมูลส่วนตัวหรือข้อมูลจราจรทางคอมพิวเตอร์ และกระบวนการนี้ไม่ได้กำหนดให้ผู้ให้บริการแจ้งบุคคลที่ถูกสอบสวนทราบ ผู้ที่ถูกสอบสวนย่อมไม่ทราบว่าตนกำลังเป็นผู้ต้องหา องค์กร Article19 จึงเสนอให้มีการแก้ไขกฎหมายเพื่อให้ศาลมีอำนาจในการตรวจสอบการใช้อำนาจตามมาตรา 18 วรรคหนึ่ง (1) - (3) และบังคับให้ผู้ให้บริการแจ้งให้บุคคลที่ถูกสอบสวนทราบ

ผู้วิจัยเห็นว่า ข้อวิจารณ์ขององค์กรนี้มีความน่าสนใจเป็นอย่างยิ่ง ในมุมมองคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของบุคคลซึ่งเป็นสิทธิที่ได้รับการรับรองตามรัฐธรรมนูญของประเทศไทย⁴⁹ แต่ผู้วิจัยเห็นว่าข้อวิจารณ์นี้ไม่ได้คำนึงว่าการใช้อำนาจของพนักงานเจ้าหน้าที่ ๖ เป็นการสืบสวนเพื่อหาตัวผู้กระทำความผิดโดยขอข้อมูลจาก “ผู้ให้บริการในฐานะพยาน” เมื่อพิจารณาตามมาตรา 132(3) ของประมวลกฎหมายวิธีพิจารณาความอาญาจะพบว่า พนักงานสอบสวนมีอำนาจออกหมายเรียกบุคคลซึ่งครอบครองสิ่งของซึ่งอาจใช้เป็น

⁴⁶ Ghazi-Tehrani (n38) 19-20; Tiprapakool and others (n 43) 9368.

⁴⁷ Article19 เป็นองค์กรที่นำชื่อมาจาก Article19 (มาตรา 19) ของ the Universal Declaration of Human Rights (ปฏิญญาสากลว่าด้วยสิทธิมนุษยชน) ซึ่งมุ่งหมายที่จะสนับสนุนสิทธิในการแสดงออกอย่างเสรี (right of freedom of expression)

⁴⁸ Article19, ‘Thailand Computer Crime Act’ (Article19, January 2017)

<<https://www.article19.org/data/files/medialibrary/38615/Analysis-Thailand-Computer-Crime-Act-31-Jan-17.pdf>> accessed 11 August 2025, 21-22.

⁴⁹ รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 มาตรา 32.

พยานหลักฐานได้ โดยที่ไม่ต้องขออนุญาตศาลเสียก่อน ดังนั้น การที่พนักงานเจ้าหน้าที่ตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ต้องการข้อมูลจากผู้ให้บริการในฐานะพยานจึงสอดคล้องกับหลักกฎหมายปัจจุบันของประเทศไทย จึงไม่มีความจำเป็นที่ต้องขออนุญาตศาลเสียก่อนเช่นกัน อย่างไรก็ตาม ข้อวิจารณ์นี้ชี้ประเด็นว่าในบริบทของการสื่อสารทางออนไลน์ กฎหมายไทยควรต้องคำนึงถึงการคุ้มครองสิทธิความเป็นอยู่ส่วนตัวด้วยหรือไม่

ตามกระบวนการของกฎหมายไทยจะเห็นได้ว่า กฎหมายไทยยังคงมีปัญหาในการหาตัวผู้หมิ่นประมาทโดยนิรนาม ด้วยเหตุนี้เอง ผู้วิจัยจะนำเสนอกระบวนการที่กฎหมายสหรัฐอเมริกาใช้ในการหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนาม เพื่อเสนอแนะในการปรับปรุงกฎหมายไทย

3. กระบวนการทางกฎหมายในการหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนามในประเทศสหรัฐอเมริกา

ในส่วนนี้ในหัวข้อที่ 3.1 ผู้วิจัยจะเริ่มอธิบายจากภาพรวมของการดำเนินคดีหมิ่นประมาทตามกฎหมายสหรัฐอเมริกาซึ่งเน้นไปที่การดำเนินคดีแพ่ง และในบริบทของการดำเนินคดีหมิ่นประมาททางออนไลน์ ผู้เสียหายไม่สามารถฟ้องผู้ให้บริการอินเทอร์เน็ตได้ เพราะมาตรา 230 ของ Communications Decency Act ('CDA') คุ้มครองผู้ให้บริการจากความรับผิดชอบที่เกิดจากเนื้อหาของผู้ใช้บริการ ผู้เสียหายจึงต้องฟ้องคดีผู้ใช้อินเทอร์เน็ตที่เป็นผู้หมิ่นประมาท ในหัวข้อที่ 3.2 ผู้วิจัยจะอธิบายหลักกฎหมายที่เกี่ยวข้องกับการขอให้เปิดเผยตัวผู้หมิ่นประมาทรวมถึงความเห็นทางวิชาการที่น่าสนใจเกี่ยวกับหลักกฎหมายนั้น

3.1 ภาพรวมของการดำเนินคดีหมิ่นประมาทในประเทศสหรัฐอเมริกา

การดำเนินคดีหมิ่นประมาทในประเทศสหรัฐอเมริกามุ่งเน้นไปที่การดำเนินคดีแพ่งเป็นหลัก ตามที่ Brenner ได้อธิบายว่า ประเทศสหรัฐอเมริกาได้รับแนวความคิดเรื่องการหมิ่นประมาททางอาญา (Criminal Libel) มาจากกฎหมาย Common Law ของประเทศอังกฤษ⁵⁰ แต่การดำเนินคดีอาญาในฐานนี้ไม่ค่อยได้มีการใช้ในประเทศสหรัฐอเมริกา⁵¹ นอกจากนี้ ศาลสูงสุดของประเทศสหรัฐอเมริกายังได้เคยวินิจฉัยในคดี *Garrison v State of Louisiana*⁵² ว่า กฎหมายระดับมลรัฐที่กำหนดโทษอาญาจากหมิ่นประมาท (Criminal Libel) ขัดต่อรัฐธรรมนูญของประเทศสหรัฐอเมริกาที่ให้ความคุ้มครองเสรีภาพในการสื่อสาร (Free Speech)⁵³ ด้วยเหตุนี้เอง นักวิชาการในประเทศสหรัฐอเมริกาจึงมีความเห็นว่า ความผิดฐานหมิ่นประมาททางอาญากำลังจะหมดจากกฎหมายสหรัฐอเมริกา⁵⁴

⁵⁰ Susan W Brenner, 'Should Online Defamation Be Criminalized?' (2007) 76 Miss LJ <<https://ssrn.com/abstract=982418>> accessed 20 April 2026.

⁵¹ *ibid* (Brenner ได้อ้างถึงข้อมูลทางสถิติของคดีหมิ่นประมาททางอาญาในประเทศสหรัฐอเมริการว่า คดีหมิ่นประมาททางอาญามีจำนวนไม่มาก).

⁵² *Garrison v. Louisiana*, 379 U.S. 64 (1964).

⁵³ *ibid* 65-66.

⁵⁴ Brenner (n 50) 10 (อ้างถึงคดี Mark W Freel, Note, *Grand Jury Subpoena and The Threat to Free Speech: In Re Grand Jury Matter (Gronowicz)*, 18 Conn L Rev 665, 684 n 109 (1986).

ในส่วนของการดำเนินคดีหมิ่นประมาททางแพ่งตามกฎหมายสหรัฐอเมริกาที่มีลักษณะเฉพาะซึ่งเป็นผลจากคำพิพากษาศาลสูงสุด ในคดี *New York Times v Sullivan* ('Sullivan') (1964)⁵⁵ ซึ่งเป็นคดีที่เจ้าหน้าที่ของรัฐ (Public Official) เรียกค่าเสียหายจาก *New York Times* เพราะมีข้อความหมิ่นประมาทปรากฏในหนังสือพิมพ์ คดีนี้ศาลสูงสุดซึ่งเห็นว่า กฎหมายมลรัฐ Alabama ที่กำหนดให้บุคคลที่วิจารณ์เจ้าหน้าที่ของรัฐต้องรับผิดชอบทางแพ่งเป็นกฎหมายที่ขัดขวางการสื่อสารทางการเมือง (Political Speech) ที่ได้รับความคุ้มครองในฐานะเสรีภาพในการสื่อสารตามรัฐธรรมนูญ กฎหมายมลรัฐ Alabama นี้จึงขัดรัฐธรรมนูญ เจ้าหน้าที่ของรัฐจึงไม่สามารถเรียกค่าเสียหายจากการหมิ่นประมาทจากการกระทำหน้าที่ของตนได้ เว้นแต่เจ้าหน้าที่ของรัฐสามารถพิสูจน์ได้ว่า ข้อความหมิ่นประมาทนั้นได้กระทำโดยมีองค์ประกอบภายใน (Actual Malice) กล่าวคือ จำเลยได้รู้อยู่แล้วว่า ข้อความนั้นเป็นเท็จหรือจำเลยไม่ได้สนใจว่าข้อความนั้นเป็นเท็จหรือไม่⁵⁶

Pantazis ได้อธิบายว่า บรรทัดฐานคดี *Sullivan* ทำให้เงื่อนไขการฟ้องคดีหมิ่นประมาทที่มีโจทก์เป็นเจ้าหน้าที่ของรัฐ (Public Officials) กับเป็นบุคคลธรรมดา (Private Persons) แตกต่างกัน เพราะเจ้าหน้าที่ของรัฐเรียกค่าเสียหายได้เฉพาะกรณีที่สามารถพิสูจน์ได้ว่า จำเลยเผยแพร่ข้อความที่หมิ่นประมาทโดยมีองค์ประกอบภายใน⁵⁷ และยังได้อธิบายต่อไปอีกว่า ศาลสูงสุดได้ขยายความต่อไปอีกในคดี *Curtis Publishing Co v Butts* (1967)⁵⁸ ว่า บุคคลสาธารณะ (Public Figures) ต้องพิสูจน์องค์ประกอบภายในเช่นกัน เพราะบุคคลสาธารณะมีความคล้ายคลึงกับเจ้าหน้าที่ของรัฐเพราะมีบทบาทที่สำคัญในสังคม และสามารถเข้าถึงสื่อมวลชนเพื่อปกป้องชื่อเสียงของตนเองได้⁵⁹ และต่อมาในคดี *Gertz v Robert Welch* (1974) ศาลปฏิเสธที่จะขยายเงื่อนไขการพิสูจน์องค์ประกอบภายในสำหรับกรณีที่โจทก์เป็นบุคคลธรรมดา เหตุผลประการหนึ่งที่ศาลใช้ คือ บุคคลธรรมดาไม่มีสื่อที่ใช้ตอบโต้เพื่อคุ้มครองชื่อเสียงของตนเหมือนกับบุคคลสาธารณะ รัฐจึงมุ่งเยียวยาความเสียหายของบุคคลธรรมดามากกว่าความเสียหายที่เกิดกับบุคคลสาธารณะ⁶⁰

นอกจากนี้ ในกรณีการหมิ่นประมาททางออนไลน์มีลักษณะเฉพาะอีกประการหนึ่ง คือ ผู้เสียหายไม่สามารถฟ้องผู้ให้บริการให้รับผิดชอบจากการที่ผู้ใช้บริการหมิ่นประมาทผู้เสียหายได้ เพราะมาตรา 230(c)(1) CDA ได้ให้ความคุ้มครองไว้ มาตรฐานนี้มีเนื้อหาแปลเป็นภาษาไทยได้ว่า

⁵⁵ *New York Times Co v Sullivan* 376 US 254 (1964) ('Sullivan').

⁵⁶ *ibid* 279-280.

⁵⁷ Annemarie Pantazis, 'Zeran v America Online, Inc: Insulating Internet Service Providers from Defamation Liability' (1999) 34 Wake Forest Law Review 531, 537-538 อ้างถึง *Sullivan* (n55) 283-84.

⁵⁸ *Curtis Publishing Co v Butts* 388 US 130 (1967) ('Curtis').

⁵⁹ Pantazis (n57) 539 อ้างถึง *Curtis* (n58) หน้า 154-55.

⁶⁰ *ibid* 539; สำหรับผู้ที่สนใจรายละเอียดเกี่ยวกับขอบเขตของบุคคลสาธารณะภายใต้กฎหมายหมิ่นประมาทของประเทศไทยสามารถศึกษาได้ที่ Nathaniel Gleicher, 'John Doe Subpoenas: Toward a Consistent Legal Standard' (2008) 118 Yale Law Journal 320, 332-334.

ผู้ให้บริการหรือผู้ใช้บริการของระบบคอมพิวเตอร์ที่ใช้ในการโต้ตอบกันจะไม่ถือเป็นผู้เผยแพร่หรือผู้กล่าวข้อมูลใด ๆ ที่ผู้อื่นเป็นผู้จัดทำขึ้น⁶¹

กฎหมายนี้เป็นกฎหมายระดับประเทศ (Federal Law) ซึ่งคุ้มครองไม่ให้ผู้ให้บริการต้องรับผิดชอบทางแพ่งจากเนื้อหาของผู้ใช้บริการ ไม่ว่าจะเป็นการหมิ่นประมาท⁶² หรือเนื้อหาที่ผิดกฎหมายอื่น ๆ⁶³ ผู้เสียหายจึงต้องดำเนินคดีบุคคลที่เขียนข้อความที่หมิ่นประมาทเป็นหลัก⁶⁴

3.2 การหาตัวผู้หมิ่นประมาทตามกฎหมายสหรัฐอเมริกา: การขังน้ำหนักระหว่างสิทธิในการสื่อสารโดยนิรนามและสิทธิในชื่อเสียงของบุคคล

ในกรณีที่ผู้เสียหายถูกหมิ่นประมาททางออนไลน์โดยนิรนาม กฎหมายสหรัฐอเมริกาได้ให้สิทธิผู้เสียหายยื่นคำร้องต่อศาล เพื่อให้มีคำสั่งให้ผู้ให้บริการอินเทอร์เน็ตเปิดเผยตัวผู้หมิ่นประมาทได้ Shuntich และ Vogel ได้อธิบายว่า กระบวนการทางกฎหมายในการหาตัวผู้หมิ่นประมาทมี 2 ขั้นตอน⁶⁵ สรุปได้ ดังนี้

ขั้นตอนแรก โจทก์จะทำการฟ้องจำเลยซึ่งไม่ทราบชื่อ (John Does)⁶⁶ และโจทก์ต้องขอให้ศาลออกหมายเรียกพยานให้นำเอกสารหรือวัตถุมาส่งศาล (*subpoenas duces tecum*) โดยส่งไปยังบริษัทหรือบุคคลที่น่าจะมีข้อมูลเกี่ยวกับจำเลยไม่ทราบชื่อ เช่น บริษัทที่ให้บริการ Social Media ต่าง ๆ หรือ ผู้ให้บริการจด Domain Name เป็นต้น ข้อมูลที่โจทก์จะได้มา คือ “ข้อมูลพื้นฐานของสมาชิก (Basic Subscriber Information)” ซึ่งคือ “ที่อยู่ เบอร์โทรศัพท์ ที่อยู่อีเมล ชื่อบัญชีสำหรับการกู้คืน และ IP Address” ทั้งนี้ แม้ผู้หมิ่นประมาทโดยนิรนามใช้ข้อมูลปลอม เช่น ที่อยู่ปลอม แต่ข้อมูลที่สำคัญที่โจทก์สามารถขอได้ คือ “บันทึกข้อมูลหมายเลข IP Address ของผู้ใช้ (users’ IP Address Log)” โดย IP Address คือ ที่อยู่ซึ่งผู้ให้บริการอินเทอร์เน็ตได้กำหนดไว้สำหรับเครื่องคอมพิวเตอร์หรืออุปกรณ์อื่นที่ใช้เชื่อมต่อเข้าสู่อินเทอร์เน็ต⁶⁷

ขั้นตอนที่ 2 เมื่อโจทก์ได้รับบันทึกข้อมูลหมายเลข IP Address โจทก์ต้องยื่นคำร้องอีกฉบับเพื่อขอให้ศาลสั่งให้ผู้ให้บริการอินเทอร์เน็ตที่กำหนดหมายเลข IP Address สำหรับเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้เชื่อมต่ออินเทอร์เน็ตเพื่อเปิดเผยว่า ใครคือผู้ใช้ IP Address นี้⁶⁸

⁶¹ No provider of user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.; สำหรับผู้สนใจเกี่ยวกับการใช้มาตรา 230 CDA สามารถศึกษารายละเอียดได้ที่ Gregory M Dickinson, ‘Section 230: A Juridical History’ (2024) 28 Stanford Technology Law Review 1.

⁶² ตัวอย่างเช่น คดี *Zeran v American Online* 129 F3d 327 (4th Cir 1997).

⁶³ ตัวอย่างเช่น คดี *Force v Facebook*, 934 F3d 53 (2019).

⁶⁴ Jessica L Chilson, ‘Unmasking John Doe: Setting a Standard for Discovery in Anonymous Internet Defamation Cases’ (2009) 95 Virginia Law Review 389, 401.

⁶⁵ Savanna L Shuntich and Kenneth A Vogel, ‘Doe Hunting: A How-To Guide for Uncovering John Doe Defendants in Anonymous Online Defamation Suits’ (2018) 35 Computer and Internet Lawyer 17, 18-19; นอกจากนี้โปรดดู Gleicher (n60) หน้า 328 (อธิบายว่า กระบวนการเปิดเผยตัวผู้ใช้อินเทอร์เน็ตนิรนามมี 2 ขั้นตอนเช่นกัน).

⁶⁶ Gleicher (n60) 327 อธิบายว่า การฟ้องคดีคู่ความที่เป็นชื่อสมมติ (fictitious parties) มีมาเป็นเวลานานแล้ว.

⁶⁷ Shuntich and Vogel (n65) 18-19.

⁶⁸ *ibid* 19.

ในกระบวนการหาตัวผู้หมิ่นประมาทนี้ Gleicher ได้ตั้งข้อสังเกตว่า ผู้ให้บริการอินเทอร์เน็ตอาจแจ้งให้จำเลยซึ่งไม่ทราบชื่อว่า มีคำร้องเพื่อให้ขอเปิดเผยตัวโดยจำเลยสามารถยื่นคำร้องคัดค้าน โดยไม่ได้เปิดเผยตัวตนต่อศาลเพื่อขอให้ศาลยกคำร้องได้⁶⁹ และกระบวนการนี้สามารถนำไปเปิดเผยตัวบุคคลที่กระทำการไม่ชอบด้วยกฎหมายอย่างอื่น เช่น คดีละเมิดเครื่องหมายการค้าได้⁷⁰ หรือ ใช้เพื่อขอให้เปิดเผยตัวผู้ใช้อินเทอร์เน็ตนิรนามในฐานะพยานในคดีได้⁷¹

ตามที่ได้กล่าวไปในบทนำว่า สิทธิในการสื่อสารโดยนิรนามถือเป็นส่วนหนึ่งของเสรีภาพในการสื่อสารตามกฎหมายสหรัฐอเมริกา⁷² นอกจากนี้ ศาลในประเทศสหรัฐอเมริกายังรับรองด้วยว่า เสรีภาพในการสื่อสารนี้รวมไปถึงการสื่อสารโดยนิรนามผ่านทางอินเทอร์เน็ตด้วย⁷³ ด้วยเหตุนี้เอง ศาลจึงได้กำหนดมาตรฐานที่โจทก์ต้องพิสูจน์ เพื่อเปิดเผยตัวจำเลยซึ่งไม่ทราบชื่อโดยนำเสรีภาพในการสื่อสารมาร่วมพิจารณาด้วย อย่างไรก็ตาม จากการศึกษาวรรณกรรมทางกฎหมาย (Legal Literature) ที่เกี่ยวข้องกับแนวทางในการเปิดเผยตัวผู้สื่อสารโดยนิรนามตามกฎหมายสหรัฐอเมริกา ผู้วิจัยพบว่า ศาลได้กำหนดมาตรฐานที่โจทก์ต้องพิสูจน์แตกต่างกันในแต่ละคดีและให้ความเห็นว่า ยังไม่ได้มีมาตรฐานที่ชัดเจน⁷⁴ แม้มาตรฐานเหล่านี้จะยังไม่ชัดเจน แต่ผู้วิจัยเห็นว่าการศึกษามาตรฐานเหล่านี้จะทำให้เห็นแนวคิดที่ศาลในประเทศสหรัฐอเมริกาใช้ เพื่อนำไปปรับให้สอดคล้องกับบริบทของกฎหมายไทยได้ ดังนั้น ในหัวข้อ 3.2.1 ผู้วิจัยจะนำเสนอมาตรฐานที่น่าสนใจ ที่ศาลในประเทศสหรัฐอเมริกาได้เคยใช้รวมไปถึงความเห็นทางวิชาการต่อมาตรฐานเหล่านั้น และในหัวข้อ 3.2.2 จะนำเสนอข้อเสนอทางวิชาการที่น่าสนใจในการพัฒนามาตรฐานที่โจทก์ต้องพิสูจน์ให้ชัดเจน

3.2.1 มาตรฐานในการพิสูจน์ของศาลในประเทศสหรัฐอเมริกา

Arbatman และ Villasenor ได้สรุปพัฒนาการของมาตรฐานที่ศาลในประเทศสหรัฐอเมริกาเคยใช้ในการเปิดเผยตัวผู้สื่อสารโดยนิรนามโดยเริ่มจากคดี *Columbia Insurance Co v Seescandy.com*⁷⁵ (1999) (*'Seescandy.com'*) ซึ่งเป็นคดีแรกที่มีการดำเนินคดีแพ่งเพื่อเปิดเผยตัวผู้สื่อสารโดยนิรนามทางอินเทอร์เน็ต⁷⁶ คดีนี้เป็นคดีละเมิดเครื่องหมายการค้า⁷⁷ ศาลกำหนดว่าโจทก์จะต้องพิสูจน์ข้อเท็จจริงดังต่อไปนี้ (1) โจทก์ต้องระบุตัวตนของบุคคลที่ยังไม่ทราบชื่อโดยเฉพาะเจาะจงให้เพียงพอ เพื่อให้ศาลสามารถพิจารณาได้

⁶⁹ Gleicher (n60) 328.

⁷⁰ *ibid* 331; see eg *Columbia Insurance Co v Seescandy.com*, 185 FRD 573 (ND Cal 1999), which will be discussed in n 77–80.

⁷¹ See *Doe v 2TheMart.com Inc*, 140 F Supp 2d 1088 (WD Wash 2001).

⁷² เจริญพร 25.

⁷³ Shuntich and Vogel (n65) 19 อ้างถึงคดี *Hard Drive Prods, Inc v Doe* 892 F Supp 2d 334, 338 (DDC 2012).

⁷⁴ Gleicher (n60) 325 (กล่าวว่า ‘คำร้องขอเปิดเผยตัวจำเลยซึ่งไม่ทราบชื่อไม่ได้มีมาตรฐานการพิสูจน์เพียงมาตรฐานเดียว’); Shuntich และ Vogel (n65) 19 (กล่าวว่า ‘ศาลในประเทศสหรัฐอเมริกายังไม่มีข้อยุติว่าการคุ้มครองสิทธิในการสื่อสารโดยนิรนามเป็นอย่างไร’); Leeza Arbatman and John Villasenor, ‘Anonymous Expression and “Unmasking” in Civil and Criminal Proceedings’ (2021) 23 Minnesota Journal of Law, Science and Technology 77, 78 (กล่าวว่า ‘แม้มีการดำเนินคดีเกี่ยวกับการเปิดเผยตัวผู้ใช้อินเทอร์เน็ตโดยนิรนามเป็นเวลากว่า 20 ปี แต่ศาลยังไม่ได้กำหนดมาตรฐานที่ชัดเจน’).

⁷⁵ *Columbia Insurance Co v Seescandy.com*, 185 FRD 573 (ND Cal 1999).

⁷⁶ Arbatman and Villasenor (n74) 99.

⁷⁷ *Columbia Insurance Co* (n77).

ว่า จำเลยเป็นบุคคลหรือนิติบุคคลที่มีตัวตนอยู่จริง และสามารถถูกฟ้องคดีในศาลได้ (2) โจทก์ต้องระบุขั้นตอนที่ได้กระทำไปโดยสุจริตในการหาที่อยู่ของจำเลย เพื่อรับประกันว่าได้มีการกระทำโดยสุจริตในการระบุตัวตนเพื่อส่งหมายไปยังจำเลย และ (3) โจทก์ต้องแสดงได้ว่าคำฟ้องของโจทก์สามารถโต้แย้งคำร้องขอให้ยกฟ้องได้⁷⁸ ต่อมาคือ คดี *In re Subpoena Duces Tecum to American Online*⁷⁹ (2001) ('AOL') ในคดีนี้ศาลมลรัฐ Virginia ได้พิจารณาคำร้องของบริษัทหนึ่ง ซึ่งฟ้องบุคคลที่โพสต์ข้อความหมิ่นประมาทตนในห้องแชทของ American Online แต่ American Online ได้ยื่นคำร้องคัดค้าน ศาล Virginia ได้กำหนดมาตรฐานว่า ผู้ให้บริการแพลตฟอร์มต้องเปิดเผยตัวผู้ให้บริการนิรนาม หาก (1) ศาลเห็นชอบตามคำขอ หรือ หลักฐานที่ยื่นมาต่อศาลว่า (2) คู่ความที่ขอยกศาลมีเหตุผลโดยสุจริตโดยชอบธรรมในการอ้างว่า ตนเสียหายจากการกระทำที่มีการฟ้องคดี และ (3) ข้อมูลของตัวบุคคลตามหมายศาลที่ขอมีความสำคัญในการดำเนินคดีต่อไป⁸⁰ ทั้งมาตรฐานจากคดี *Seescandy.com* และ AOL นี้ถูกวิจารณ์ว่า ไม่ได้ให้ความคุ้มครองสิทธิในการสื่อสารโดยนิรนามเท่าใดนัก⁸¹

Arbatman และ Villasenor ได้อธิบายต่อว่า เนื่องจากมาตรฐานของทั้งสองคดีไม่ได้คำนึงถึงสิทธิในการสื่อสารโดยนิรนามเท่าใด ศาลในมลรัฐอื่นจึงกำหนดมาตรฐานใหม่ให้โจทก์ต้องพิสูจน์⁸² เช่น ศาล New Jersey Appellate Court ในคดี *Dendrite International, Inc v Doe No 3*⁸³ (2001) ('Dendrite') ได้กำหนดว่าโจทก์ต้องพิสูจน์ว่า (1) โจทก์ได้แจ้งไปยังจำเลยซึ่งไม่ทราบชื่อ ทั้งนี้ สามารถแจ้งโดยโพสต์ไปยังเว็บไซต์ที่จำเลยได้หมิ่นประมาทว่า โจทก์กำลังขอยกศาลเพื่อเปิดเผยตัว และต้องใช้เวลาตามควรแก่จำเลยในการโต้แย้งคำขอ (2) ระบุข้อความที่โจทก์อ้างว่าหมิ่นประมาท และ (3) ต้องสามารถแสดงได้ว่าคดีของโจทก์มีมูล (*prima facie*)⁸⁴ และหากศาลเห็นว่า โจทก์ได้แสดงต่อศาลว่าได้ดำเนินการตามที่กล่าวมาแล้ว (4) ศาลต้องชั่งน้ำหนักระหว่างการคุ้มครองสิทธิของผู้ที่สื่อสารโดยนิรนามกับความน่าเชื่อถือของคำฟ้องโจทก์ เพื่อพิจารณาว่าควรเปิดเผยตัวตนของจำเลยหรือไม่⁸⁵

ภายหลังจากคดี *Dendrite* ได้มีคดี *Doe v Cahill*⁸⁶ (2005) ('Cahill') ของศาล Delaware Supreme Court โจทก์ในคดีนี้เป็นบุคคลสาธารณะซึ่งต่างจากคดีอื่น ๆ ที่โจทก์เป็นบริษัทที่ถูกหมิ่นประมาท⁸⁷ ศาล Delaware ได้ปรับปรุงมาตรฐานจากคดี *Dendrite* ให้เหลือ 2 ข้อ กล่าวคือ (1) โจทก์ยังคงต้องพยายามแจ้งผู้ใช้อินเทอร์เน็ตนิรนามเหมือนกับคดี *Dendrite* และ (2) โจทก์ต้องแสดงข้อเท็จจริงที่เพียงพอต่อการโต้แย้งคำร้องขอให้ศาลมีคำพิพากษาโดยไม่ต้องสืบพยาน (Summary Judgment Motion) ศาลได้อธิบายว่า โจทก์ต้องนำเสนอหลักฐานที่เป็นประเด็นสำคัญสำหรับทุกองค์ประกอบที่โจทก์สามารถพิสูจน์ได้ (Within

⁷⁸ *ibid.*

⁷⁹ *In re Subpoena Duces Tecum to America Online, Inc*, 2000 WL 1210372 (Cir Ct Va 2000).

⁸⁰ *ibid* 8.

⁸¹ Gleicher (n60) 340; Arbatman and Villasenor (n74) 99.

⁸² Arbatman and Villasenor (n74) 99.

⁸³ *Dendrite International, Inc v Doe No 3*, 342 NJ Super 134, 775 A2d 756 (App Div 2001).

⁸⁴ *ibid* 760.

⁸⁵ *ibid* 760-761.

⁸⁶ *CML V, LLC v Bax*, 884 A2d 451 (Del 2005).

⁸⁷ *ibid* 454.

the Plaintiff's Control)⁸⁸ เพราะเมื่อโจทก์ในคดีนี้เป็นบุคคลสาธารณะ โจทก์จึงต้องพิสูจน์ว่า **ผู้ใช้อินเทอร์เน็ตโดยนิรนามได้หมิ่นประมาทโดยมีองค์ประกอบภายใน** แต่ศาลเห็นว่า เป็นเรื่องยากที่โจทก์จะพิสูจน์ได้ หากโจทก์ไม่ทราบว่าเป็นใครคือผู้ใช้อินเทอร์เน็ตคนนั้น ดังนั้น โจทก์จึงไม่ต้องพิสูจน์องค์ประกอบนี้ ทั้งนี้ ศาลได้อธิบายว่า การกำหนดให้โจทก์ต้องระบุข้อความที่อ้างว่าหมิ่นประมาทตามองค์ประกอบข้อ 2 ของคดี *Dendrite*⁸⁹ และการกำหนดให้ศาลต้องชั่งน้ำหนักตามองค์ประกอบข้อ 4 ของคดี *Dendrite* อยู่ในกระบวนการพิจารณาการโต้แย้งคำร้องนี้อยู่แล้ว⁹⁰

มาตรฐานของคดี *Dendrite* และ *Cahill* นี้ได้รับการชื่นชมว่า เป็นมาตรฐานที่เหมาะสมในการชั่งน้ำหนักระหว่างสิทธิในการสื่อสารโดยนิรนามของผู้พูดกับสิทธิของโจทก์ที่จะได้รับการเยียวยาความเสียหาย จากข้อความหมิ่นประมาทโดยกระบวนการทางศาล⁹¹

คดีสุดท้ายที่ Arbatman และ Villasenor กล่าวถึงเกี่ยวกับการเปิดเผยตัวในคดีแพ่ง คือ คดี *In re Anonymous Speakers*⁹² (2011) ซึ่งวินิจฉัยโดย ศาล Ninth Circuit ศาลเห็นว่ามาตรฐานของคดี *Cahill* กว้างเกินไป เพราะศาลเห็นว่าลักษณะของการสื่อสาร (Nature of Speech) ควรเป็นประเด็นหลักที่ใช้ในการให้น้ำหนักสำหรับการสื่อสารโดยนิรนามในกระบวนการเปิดเผยตัวผู้ใช้อินเทอร์เน็ต ศาลได้อธิบายว่าการสื่อสารที่เกี่ยวกับเรื่องทางพาณิชย์ (Commercial Speech) ได้รับความคุ้มครองในฐานะเสรีภาพในการสื่อสารน้อยกว่าการสื่อสารเรื่องการเมือง ทั้งนี้ Arbatman และ Villasenor ได้อธิบายว่าหลังจากคดี *Anonymous Speakers* แล้ว ยังไม่มีความชัดเจนว่า มาตรฐานในการพิสูจน์เพื่อเปิดเผยตัวผู้สื่อสารโดยนิรนามตามลักษณะของการสื่อสารแต่ละประเภทควรจะเป็นอย่างไร⁹³

3.2.2 ข้อเสนอทางวิชาการเกี่ยวกับมาตรฐานในการพิสูจน์

เนื่องจากกฎหมายสหรัฐอเมริกายังไม่มีความชัดเจนถึงมาตรฐานที่โจทก์ต้องพิสูจน์ จึงมีความเห็นทางวิชาการที่นำเสนอมาตรฐานที่น่าสนใจให้ศาลในประเทศสหรัฐอเมริกานำไปใช้ เช่น Gleicher เห็นว่า โจทก์จะต้องพิสูจน์ 4 ประเด็น ดังต่อไปนี้ (1) โจทก์ และผู้ให้บริการที่ถูกหมายเรียกได้ใช้ความพยายามตามสมควรในการแจ้งให้จำเลยซึ่งไม่ทราบชื่อ (2) โจทก์ต้องพิสูจน์ถึงความน่าเชื่อถือของคำฟ้องโจทก์⁹⁴ ทั้งนี้ ตามที่ได้กล่าวไปข้างต้นว่า การฟ้องคดีโดยโจทก์ที่เป็นบุคคลธรรมดาที่มีองค์ประกอบที่แตกต่างจากการฟ้องคดีโดยโจทก์ที่เป็นบุคคลสาธารณะ เพราะบุคคลสาธารณะต้องพิสูจน์องค์ประกอบภายใน⁹⁵ Gleicher ได้อธิบายว่า หากโจทก์เป็นบุคคลธรรมดา โจทก์ต้องนำเสนอหลักฐานเพื่อพิสูจน์ว่าจำเลยหมิ่นประมาทตนในระดับที่แสดงว่าคดีมีมูล (Prima Facie) แต่หากโจทก์เป็นบุคคลสาธารณะที่ฟ้องคดีหมิ่นประมาท ในประเด็นที่เป็น

⁸⁸ ibid 464.

⁸⁹ ibid 461.

⁹⁰ ibid.

⁹¹ Gleicher (n60) 340; Shuntich and Vogel (n65) 19.

⁹² Arbatman and Villasenor (n74) 103 (อ้างถึงคดี *In re Anonymous Speakers* 661 F3d 1168 (9th Cir 2011)).

⁹³ นอกจากคดีที่กล่าวมานี้ Arbatman และ Villasenor ยังได้อ้างถึงคดี *Doe v 2Mart.com* (2001) ซึ่งเป็นเรื่องเกี่ยวกับการเปิดเผยตัวพยานซึ่งเป็นผู้ใช้อินเทอร์เน็ตโดยนิรนาม รายละเอียดโปรดดู ibid 102.

⁹⁴ Gleicher (n60) 363.

⁹⁵ โปรดดู เนื้อหาของเชิงอรรถที่ 55-60.

สาธารณะ (Public Speech) โจทก์ต้องนำเสนอหลักฐานที่โจทก์สามารถพิสูจน์ได้ ทั้งนี้ เพราะการพิสูจน์องค์ประกอบภายในของจำเลยไม่ใช่เรื่องง่าย หากไม่ทราบว่าจำเลยเป็นใคร ดังนั้น โจทก์ต้องนำเสนอข้อเท็จจริงเพื่อโน้มน้าวศาลว่าจำเลยได้กระทำโดยมีองค์ประกอบภายใน (3) โจทก์ต้องแสดงให้เห็นว่า ข้อมูลที่โจทก์ร้องขอนั้นมีความจำเป็นในการระบุตัวจำเลย และตัวจำเลยเป็นสาระสำคัญในการดำเนินคดี และ (4) หากการพิจารณาทั้งสามองค์ประกอบข้างต้นยังไม่สามารถสรุปได้ว่าให้เปิดเผยตัวหรือไม่ ศาลต้องชั่งน้ำหนักระหว่างประโยชน์ของคู่ความโดยให้พิจารณาว่าความเสียหายจะเกิดขึ้นกับฝ่ายใดมากกว่ากัน⁹⁶

จะเห็นได้ว่า ข้อเสนอของ Gleicher เป็นการทำให้มาตรฐานคดี *Cahill* มีความชัดเจนขึ้น ในประเด็นที่บุคคลสาธารณะต้องพิสูจน์องค์ประกอบภายใน และมีการกำหนดให้ศาลนำเรื่องการชั่งน้ำหนักมาร่วมพิจารณาให้ชัดเจนขึ้น

ในส่วนของ Arbatman และ Villasenor ได้เสนอว่า ควรนำมาตรฐานการพิสูจน์ในคดี *Dendrite* มาใช้เพราะมีการกำหนดให้ศาลพิจารณาว่า (1) คดีมีมูลมากเพียงใด (The Strength of The *prima facie* Case) และ (2) ให้มีการชั่งน้ำหนักระหว่าง ความจำเป็นในการเปิดเผยตัวจำเลยซึ่งไม่ทราบชื่อเพื่อให้โจทก์ดำเนินคดี กับ สิทธิในการสื่อสารโดยนิรนามซึ่งได้รับความคุ้มครองตามรัฐธรรมนูญ⁹⁷ ดังนั้น จึงเสนอให้นำมาตรฐานทั้ง 4 ข้อของคดี *Dendrite* ไปใช้ โดยที่ Arbatman และ Villasenor ยอมรับว่า การชั่งน้ำหนักตามมาตรฐานนี้ยังมีความไม่ชัดเจนอยู่⁹⁸ จึงได้เสนอว่าควรนำ 3 ประเด็นนี้ มาร่วมพิจารณาด้วยในการชั่งน้ำหนักด้วย คือ

(1) ให้พิจารณาประเภทของการสื่อสารโดยนิรนาม (Type of Anonymous Speech) เพราะตามกฎหมายสหรัฐอเมริกา ลักษณะของการสื่อสารมีผลต่อเสรีภาพในการสื่อสารตามรัฐธรรมนูญ กล่าวคือ ศาลในประเทศสหรัฐอเมริกาให้ความสำคัญกับการสื่อสารทางการเมือง (Political Speech)⁹⁹ และการสื่อสารในงานเขียน และเรื่องทางศาสนา¹⁰⁰ แต่หากเป็นการสื่อสารที่เกี่ยวกับเรื่องเชิงพาณิชย์จะได้รับความคุ้มครองน้อยกว่า¹⁰¹ ทั้งคู่ให้ความเห็นว่า หากศาลพิจารณาแล้วเห็นว่าการสื่อสารนั้นเป็นเรื่องการเมือง งานเขียน หรือ เรื่องศาสนา ให้ศาลมีคำสั่งไม่เปิดเผยตัวจำเลย แต่หากเป็นการสื่อสารทางพาณิชย์ศาลควรพิจารณาให้เปิดเผย อย่างไรก็ตาม ทั้งคู่ยอมรับว่า มาตรฐานของศาลในการพิจารณาว่าการสื่อสารใดเป็นการสื่อสารเชิงพาณิชย์ยังมีความชัดเจน¹⁰² และในบางกรณี การพิจารณาว่าการสื่อสารเป็นการสื่อสารเชิงพาณิชย์หรือไม่ จำเป็นต้องทราบว่าใครคือผู้สื่อสารด้วย¹⁰³ ทั้งคู่จึงได้เสนอว่า กรณีที่ไม่ชัดเจนว่าเป็นการสื่อสารประเภทใด หรือ หากการพิจารณาว่าการสื่อสารนั้นเป็นการสื่อสารประเภทใดต้องมีการเปิดเผยตัวผู้สื่อสาร ให้มีคำสั่งไม่เปิดเผยตัวผู้สื่อสาร

⁹⁶ Gleicher (n60) 363.

⁹⁷ Arbatman and Villasenor (n74) 122.

⁹⁸ Arbatman and Villasenor (n74) 122; นอกจากนี้ โปรดดู Chilson (n64) 414 (อธิบายว่า ‘การชั่งน้ำหนักเป็นการให้ดุลพินิจกับศาล โดยที่ไม่ได้มีแนวทางว่าโจทก์ต้องนำเสนอหลักฐานแบบใดจึงจะเป็นไปตามแนวของ คดี *Dendrite*’).

⁹⁹ Arbatman and Villasenor (n74) 122 (อ้างถึง คดี *McIntyre v Ohio Elections Commission* (n25))

¹⁰⁰ *ibid* (อ้างถึงคดี *Anonymous Speakers* (n92)).

¹⁰¹ *ibid* 124-125 (อ้างถึงคดี *Cent Hudson Gas v Pub Serv Comm’n of NY* 447 US 557, 562-63 (1980)).

¹⁰² *ibid* 127.

¹⁰³ *ibid* 126 (อ้างถึงคดี *SI03 Inc v Bodybuilding.com, LLC* 441 F App’x 431 (9th Cir 2011)).

(2) ผู้ที่สื่อสารเป็นคู่ความในคดีหรือไม่ ทั้งนี้ การเปิดเผยตัวผู้สื่อสารโดยนิรนามในประเทศสหรัฐอเมริกาสามารถนำไปใช้เพื่อขอเปิดเผยตัวพยานในคดีได้¹⁰⁴ Arbatman และ Villasenor ได้อธิบายว่า คู่ความที่ต้องการให้เปิดเผยผู้ที่สื่อสารในฐานะพยานต้องมีการพิจารณาที่สูงกว่าการขอให้เปิดเผยตัวจำเลย ศาลควรพิจารณาถึง ความสำคัญของพยานในคดีนี้เมื่อพิจารณาประกอบกับหลักฐานอื่น ๆ รวมไปถึงผลที่จะเกิดขึ้นหากมีการเปิดเผยตัวพยาน เช่น การมีคำสั่งเปิดเผยตัวเช่นนี้ จะทำให้ผู้ใช้อินเทอร์เน็ตไม่อยากจะออกความเห็นในลักษณะเดียวกันอีกหรือไม่¹⁰⁵

(3) การเปรียบเทียบว่า ความเสียหายที่อาจเกิดขึ้นกับผู้สื่อสารโดยนิรนามกับที่อาจเกิดกับผู้เสียหาย หากคำสั่งให้เปิดเผยตัวตนมีความผิดพลาด Arbatman และ Villasenor ได้ยกตัวอย่างว่า เจ้าของร้านอาหารที่ขอให้ศาลเปิดเผยตัวผู้ใช้อินเทอร์เน็ตที่รีวิว (Review) ว่าร้านอาหารคิดราคาแพงเกินเหตุ หากศาลปฏิเสธที่จะเปิดเผยตัวผู้ใช้นี้ เจ้าของร้านย่อมไม่สามารถได้รับการเยียวยาความเสียหาย เช่น ไม่สามารถทำให้บุคคลนั้นลบข้อความออกไป แต่ในทางกลับกัน หากศาลมีคำสั่งให้เปิดเผยตัว แต่เมื่อพิจารณาในเนื้อหาคดีกลับพบว่าข้อความนั้นเป็นความจริง คำสั่งนี้ย่อมละเมิดเสรีภาพในการสื่อสารโดยนิรนามที่ได้รับการรับรองตามรัฐธรรมนูญ โดย Arbatman และ Villasenor ได้อธิบายเพิ่มเติมว่า หากพิจารณาในรายละเอียดความเสียหายที่เกิดขึ้นอาจมีระดับที่ต่างกัน เช่น หากข้อเท็จจริงปรากฏว่า มีการร้องเรียนจำนวนมากว่าร้านนี้คิดราคาแพงเกินเหตุ ดังนี้ ความเสียหายที่เกิดกับจำเลยที่ถูกเปิดเผยตัวจากคำสั่งที่ผิดพลาด (เพราะการเขียนรีวิวเป็นเรื่องจริง) ย่อมมีมากกว่าความเสียหายที่จะเกิดขึ้นกับโจทก์ หากศาลยกคำร้องขอให้เปิดเผยตัว¹⁰⁶

จะเห็นได้ว่า ข้อเสนอข้างต้นทำให้วิธีการชั่งน้ำหนักในคดี *Dendrite* มีความชัดเจนขึ้น และให้ความคุ้มครองเสรีภาพในการสื่อสารค่อนข้างชัดเจน จากการที่ให้ยกคำร้องหากเป็นการสื่อสารทางการเมือง หรือกรณีที่ไม่สามารถระบุลักษณะของการสื่อสารได้ว่าเป็นการสื่อสารประเภทใด

จากพัฒนาการของมาตรฐานที่ศาลกำหนดให้โจทก์พิสูจน์และข้อเสนอทางวิชาการ ทำให้ผู้วิจัยเห็นว่า ในการพิจารณาคำร้องตามกฎหมายวิธีสบัญญัติ (Procedural Law) ในเรื่องนี้ กฎหมายสหรัฐอเมริกา นำหลักกฎหมายหมิ่นประมาทซึ่งเป็นกฎหมายสารบัญญัติ (Substantive Law) มาใช้เป็นเงื่อนไขในการพิจารณาว่าจะเปิดเผยตัวผู้ใช้อินเทอร์เน็ตหรือไม่ กล่าวคือ ในกรณีที่โจทก์เป็นบุคคลสาธารณะที่ต้องการให้มีการเปิดเผยตัวผู้ใช้อินเทอร์เน็ต โจทก์ต้องโน้มน้าวให้ศาลเห็นถึงองค์ประกอบภายในของผู้ใช้อินเทอร์เน็ตตามกฎหมายหมิ่นประมาท ศาลจึงจะมีคำสั่งให้เปิดเผยตัว นอกจากนี้กฎหมายสหรัฐอเมริกายังมีการนำเสรีภาพในการสื่อสารที่รับรองตามรัฐธรรมนูญมาพิจารณาประกอบด้วย

4. การปรับปรุงกระบวนการตามกฎหมายไทยในการหาตัวผู้หมิ่นประมาททางออนไลน์โดยนิรนาม

จากการแนวทางของกฎหมายสหรัฐอเมริกา ประเด็นที่ผู้วิจัยเห็นว่าควรนำมาใช้ในกฎหมายไทย คือ การให้สิทธิผู้เสียหายยื่นคำร้องให้ศาลสั่งให้ผู้ให้บริการเปิดเผยข้อมูลของผู้ใช้อินเทอร์เน็ตโดยนิรนามได้โดยตรง ทั้งนี้ ศาลต้องนำประเด็นดังต่อไปนี้ มาใช้ประกอบการพิจารณาเพื่อเปิดเผยตัวด้วย

- (1) ผู้เสียหายได้พยายามแจ้งให้ผู้ใช้อินเทอร์เน็ตโดยนิรนามทราบว่ามีคำร้องขอให้เปิดเผยตัว
- (2) ผู้เสียหายได้นำเสนอข้อเท็จจริงให้ศาลเห็นว่าคดีหมิ่นประมาทมีมูล

¹⁰⁴ คดี *Doe v 2Mart.com* (2001) (n71).

¹⁰⁵ Arbatman and Villasenor (n74) 128.

¹⁰⁶ *ibid* 128-129.

(3) การเปิดเผยตัวตนของผู้ใช้อินเทอร์เน็ตโดยนิรนามกระทบต่อเสรีภาพในการสื่อสารเกินสมควรหรือไม่

จากประเด็นข้างต้น ผู้วิจัยจึงเสนอให้มีการแก้ไขเพิ่มเติม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ เพื่อให้สิทธิผู้เสียหายยื่นคำร้องโดยตรงต่อศาล ให้ศาลพิจารณาว่าจะมีคำสั่งให้ผู้ให้บริการเปิดเผยข้อมูลเกี่ยวกับผู้หมิ่นประมาทโดยนิรนามหรือไม่ โดยให้เพิ่มเป็นมาตรา 18 วรรคท้าย ดังนี้

ผู้เสียหายซึ่งถูกหมิ่นประมาทมีสิทธิยื่นคำร้องต่อศาลเพื่อให้ศาลสั่งให้ผู้ให้บริการเปิดเผยข้อมูลจากรายคอมพิวเตอร์ และให้ส่งมอบข้อมูลเกี่ยวกับผู้ใช้บริการที่ต้องเก็บตามมาตรา 26 ที่มีความเกี่ยวข้องกับผู้หมิ่นประมาทผ่านระบบคอมพิวเตอร์ โดยผู้เสียหายต้องแสดงหลักฐานว่าได้แจ้งให้ผู้หมิ่นประมาททราบ หากศาลพิจารณาแล้ว เห็นว่าคำร้องของผู้เสียหายมีมูลที่จะรับฟังได้ว่ามีกระทำความผิดฐานหมิ่นประมาท ให้ศาลสั่งให้ผู้ให้บริการเปิดเผยข้อมูลนั้น แต่หากศาลพิจารณาแล้วเห็นว่าคดีไม่มีมูล หรือ การกระทำนั้นไม่เป็นความผิด ให้ศาลยกคำร้องนั้นเสีย

บทบัญญัติที่ผู้วิจัยเสนอให้แก้ไขเพิ่มเติมสามารถอธิบายได้ ดังนี้

(1) ผู้เสียหายต้องแสดงหลักฐานว่าได้แจ้งให้ผู้หมิ่นประมาททราบว่า มีคำร้องขอให้เปิดเผยตัวผู้หมิ่นประมาทเพื่อให้บุคคลนั้นมีโอกาสยื่นคำร้องคัดค้าน (โดยปกปิดตัวผู้ยื่นคำร้องคำคัดค้านได้) ทั้งนี้ ตามแนวทางของคดี *Dendrite* การที่ผู้ร้องแสดงว่าได้โพสต์ไปยังเว็บไซต์ที่จำเลยได้หมิ่นประมาทว่า โจทก์กำลังขอมายศาลเพื่อเปิดเผยตัวย่อมถือว่าการแจ้งโดยชอบ

(2) ผู้เสียหายต้องนำเสนอข้อเท็จจริงให้ศาลเห็นว่า คดีหมิ่นประมาทของผู้เสียหายมีมูล กล่าวคือ ต้องแสดงข้อเท็จจริงให้ศาลเห็นว่า ข้อความที่ผู้เสียหายอ้างถึงทำให้ผู้เสียหายเสียชื่อเสียงได้ ทั้งนี้ ตามแนวคำพิพากษาศาลฎีกา ศาลวางหลักว่า ต้องได้ความว่าการใส่ความระบุถึงตัวบุคคลได้แน่นอนว่าเป็นใคร¹⁰⁷ ดังนั้น หากข้อความนั้นไม่ชัดเจนว่าหมายถึงผู้เสียหาย ให้ศาลยกคำร้องได้ทันที เช่น ผู้ใช้อินเทอร์เน็ตใช้ข้อความว่า พระวัด ก. ประพฤติผิดศีล โดยที่วัดนี้มีพระ 200 รูป ข้อความนี้ย่อมไม่สามารถระบุได้ว่าพระรูปไหนเป็นผู้เสียหาย

ทั้งนี้ ความผิดฐานหมิ่นประมาทตามกฎหมายอาญากำหนดเพียงให้โจทก์พิสูจน์ว่าจำเลยมีเจตนา แต่ไม่ได้กำหนดให้พิสูจน์ว่าจำเลยรู้หรือควรรู้ว่า ข้อความนั้นเป็นเท็จเหมือนกับกรณีกฎหมายสหรัฐอเมริกา ดังนั้น หลักเกณฑ์ที่ *Gleicher* นำเสนอว่า ต้องแสดงข้อเท็จจริงเพื่อโน้มน้าวศาลจึงไม่ต้องนำมาใช้ในประเด็นนี้

(3) การกำหนดให้ศาลพิจารณาว่า การกระทำนั้นเป็นความผิดฐานหมิ่นประมาทหรือไม่ เป็นการกำหนดให้ศาลพิจารณาว่า การเปิดเผยตัวตนของผู้ใช้อินเทอร์เน็ตกระทบต่อเสรีภาพในการสื่อสารเกินสมควรหรือไม่ ทั้งนี้ ผู้วิจัยเห็นว่า เสรีภาพในการสื่อสารทางออนไลน์ของบุคคลในบริบทของกฎหมายไทยได้รับความคุ้มครองโดยประมวลกฎหมายอาญามาตรา 329¹⁰⁸ ที่ยกเว้นความผิดฐานหมิ่นประมาทไว้

¹⁰⁷ ตัวอย่างเช่น คำพิพากษาศาลฎีกาที่ 1513/2551, คำพิพากษาศาลฎีกาที่ 619/2517.

¹⁰⁸ ผู้วิจัยไม่ได้อ้างถึงมาตรา 331 เพราะมาตรานี้ยกเว้นความผิดในการแสดงความเห็นในศาลซึ่งไม่เกี่ยวกับการสื่อสารทางออนไลน์ และไม่ได้นำมาตรา 330 มาร่วมพิจารณาด้วย เพราะมาตรา 330 ใช้กับกรณีที่ผู้หมิ่นประมาทพิสูจน์ความจริงที่เป็นประโยชน์สาธารณะได้ ดังนั้น ผู้หมิ่นประมาทต้องเข้ามาอยู่ในกระบวนการพิจารณาเสียก่อนจึงสามารถขอพิสูจน์ความจริงได้เพื่อยกเว้นความโทษได้.

มาตรา 329 มีองค์ประกอบสำคัญที่ทำให้บุคคลไม่ต้องรับผิดชอบหมิ่นประมาท คือ “เป็นการแสดงความคิดเห็นหรือข้อความโดยสุจริต” ซึ่งบัญญัติไว้ในวรรคแรก ศาสตราจารย์ จิตติ ดิงศภัทย์ ได้อธิบายว่า หมายถึง บุคคลที่ถูกฟ้องว่าหมิ่นประมาทเชื่อโดยสุจริตว่าเป็นความจริง¹⁰⁹ ในประเด็นนี้ ผู้วิจัยเห็นว่าควรนำมาตรฐานการนำเสนอข้อเท็จจริงเพื่อโน้มน้าวศาลตามข้อเสนอของ Gleicher มาใช้ เพราะการพิสูจน์ว่า ผู้ใช้อินเทอร์เน็ตโดยนิรนามไม่ได้เชื่อโดยสุจริตไม่ใช่เรื่องง่าย คล้ายคลึงกับเรื่องการพิสูจน์องค์ประกอบภายในตามกฎหมายสหรัฐอเมริกา ดังนี้ หากผู้เสียหายนำเสนอข้อเท็จจริงเพื่อโน้มน้าวศาลว่า ผู้ใช้อินเทอร์เน็ตไม่ได้เชื่อโดยสุจริตย่อมเพียงพอ กล่าวคือ หากข้อความที่ผู้ใช้อินเทอร์เน็ตใช้ไม่ได้แสดงให้เห็นถึงการอ้างอิงแหล่งข่าวประกอบข้อความ เช่น การเขียนข้อความว่า นักการเมือง ก. มีความเกี่ยวข้องกับการก่อการร้ายโดยไม่มีข้อเท็จจริงใด ๆ ที่แสดงหลักฐานยืนยันถึงข้อเท็จจริงนั้นเลย ย่อมถือว่าเพียงพอที่จะโน้มน้าวศาลว่าจำเลยไม่ได้กระทำโดยสุจริต¹¹⁰ เป็นต้น

ในทางกลับกัน หากเป็นการวิพากษ์วิจารณ์ทางการเมืองที่มีการแสดงข้อเท็จจริงประกอบ เช่น การวิจารณ์นักการเมืองมีการเชื่อมโยงถึงข้อเท็จจริงที่ปรากฏในสื่อมวลชน ทำให้ศาลเชื่อว่า ผู้ใช้อินเทอร์เน็ตได้ติชมนักการเมืองคนนี้ด้วยความเป็นธรรม ศาลควรใช้ประเด็นนี้มาพิจารณาเพื่อปฏิเสธคำร้องขอเปิดเผยตัวผู้ใช้อินเทอร์เน็ตได้¹¹¹

การให้สิทธิผู้เสียหายยื่นคำร้องได้โดยตรง สามารถแก้ไขปัญหาที่ผู้วิจัยได้กล่าวไว้ในหัวข้อที่ 2.3 ได้ เพราะเมื่อผู้เสียหายสามารถยื่นคำร้องได้เอง จำนวนพนักงานเจ้าหน้าที่ ๆ ที่ไม่เพียงพอย่อมไม่มีผลต่อการดำเนินคดีหมิ่นประมาทอีก และเมื่อศาลเป็นองค์กรที่มีคำสั่งให้ผู้ให้บริการเปิดเผยข้อมูล ผู้ให้บริการย่อมมีความมั่นใจว่า การเปิดเผยข้อมูลตามคำสั่งศาลเป็นการกระทำที่ชอบด้วยกฎหมาย ปัญหาที่ว่าผู้ให้บริการปฏิเสธที่จะให้ความร่วมมือกับพนักงานเจ้าหน้าที่ ๆ ย่อมหมดไป การคุ้มครองสิทธิในชื่อเสียงของบุคคลตามกระบวนการนี้ย่อมมีประสิทธิภาพมากขึ้น นอกจากนี้ การให้ศาลเป็นผู้พิจารณาว่า ผู้ให้บริการต้องเปิดเผยตัวผู้ให้บริการหรือไม่ ย่อมเป็นการสร้างหลักประกันว่า สิทธิความเป็นอยู่ส่วนตัวของผู้ใช้อินเทอร์เน็ตจะได้รับ ความคุ้มครอง และจากการศึกษากฎหมายสหรัฐอเมริกายังแสดงให้เห็นอีกว่า กระบวนการนี้ให้ศาลมีส่วนในการคุ้มครองเสรีภาพในการสื่อสารของผู้ใช้อินเทอร์เน็ตโดยนิรนามด้วย สิทธิในชื่อเสียงย่อมได้รับความคุ้มครองอย่างเหมาะสมภายใต้กระบวนการนี้

แม้กระบวนการที่ผู้วิจัยเสนอให้แก้ไขเพิ่มเติมเป็นกระบวนการที่ให้สิทธิผู้เสียหายหาตัวผู้หมิ่นประมาทโดยอาศัยตาม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ ซึ่งเป็นกฎหมายอาญา แต่กระบวนการนี้ไม่ได้บังคับว่าเมื่อผู้เสียหายทราบว่าเป็นผู้หมิ่นประมาทแล้ว ผู้เสียหายต้องดำเนินคดีอาญากับบุคคลนั้น ผู้เสียหายสามารถเลือกที่จะฟ้องคดีบุคคลนั้นตามกฎหมายแพ่งก็ได้

5. บทสรุป

ตามที่ผู้วิจัยได้นำเสนอจะเห็นว่า การสื่อสารโดยนิรนามสามารถถูกใช้เป็นเครื่องมือในการหมิ่นประมาทผู้อื่นได้ และก่อให้เกิดอุปสรรคต่อผู้เสียหายในการดำเนินคดีทั้งทางอาญาและทางแพ่ง แม้กฎหมาย

¹⁰⁹ จิตติ ดิงศภัทย์, คำอธิบายประมวลกฎหมายอาญา ภาค 2 ตอน 2 และภาค 3 (พิมพ์ครั้งที่ 7 เพชรบุรี 2554) 461.

¹¹⁰ เทียบเคียงคำพิพากษาศาลฎีกาที่ 418/2567.

¹¹¹ เทียบเคียงคำพิพากษาศาลฎีกาที่ 1861/2561.

ไทยจะมีกระบวนการหาตัวผู้กระทำผิดไว้ใน พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ แต่กระบวนการมีปัญหาทางปฏิบัติ เช่น พนักงานเจ้าหน้าที่ ฯ ซึ่งต้องดำเนินการตามกฎหมายมีจำนวนไม่มาก และผู้ให้บริการอาจไม่ให้ความร่วมมือในการให้ข้อมูล ด้วยเหตุผลนี้เอง กฎหมายจึงยังไม่สามารถคุ้มครองสิทธิในชื่อเสียงของผู้เสียหายได้อย่างมีประสิทธิภาพ

จากการศึกษาแนวทางของกฎหมายสหรัฐอเมริกาเพื่อนำเสนอทางแก้ไข ผู้วิจัยเสนอให้ผู้เสียหายมีสิทธิในการร้องขอต่อศาลให้มีคำสั่งให้ผู้ให้บริการเปิดเผยตัวผู้หมิ่นประมาท โดยกำหนดเงื่อนไขให้ศาลต้องพิจารณาด้วยว่าการเปิดเผยตัวผู้หมิ่นประมาทกระทบต่อเสรีภาพในการสื่อสารเกินไปหรือไม่ โดยต้องมีการแก้ไขเพิ่มเติม พ.ร.บ. ความผิดเกี่ยวกับคอมพิวเตอร์ ฯ กระบวนการเช่นนี้สามารถแก้ไขปัญหาข้างต้นได้ นอกจากนี้ ยังทำให้ศาลได้มีบทบาทในการรับประกันว่าเสรีภาพการสื่อสารของผู้ใช้อินเทอร์เน็ตจะได้รับความคุ้มครองอย่างเหมาะสมด้วย