



พศ. ดร.นรรณ์มย์ โทมลาธุน

การให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน ในสหพันธรัฐเยอรมนี

สถาบันพระปกเกล้า

รหัสสิ่งพิมพ์ของสถาบันพระปกเกล้า สสว. 62-27-00.0 (e-book)
เลขมาตรฐานสากลประจำหนังสือ 978-616-476-046-2

พิมพ์ครั้งที่ 1 กรกฎาคม 2562

บรรณาธิการ นางสาวชมพูนุท ตั้งถาวร
ประสานงาน นางสาววัชรรา เชิงหอม

จัดทำโดย

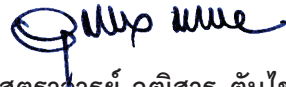
สถาบันพระปกเกล้า
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา
อาคารรัฐประศาสนภักดี ชั้น 5 ฝั่งทิศใต้
เลขที่ 120 หมู่ 3 ถนนแจ้งวัฒนะ
แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210
<http://www.kpi.ac.th>

คำนำ

รัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560 ได้บัญญัติรับรองให้บุคคลมีเสรีภาพในการติดต่อสื่อสารถึงกัน และกำหนดให้การตรวจ การกัก หรือการเปิดเผยข้อมูลที่บุคคลสื่อสารถึงกันนั้น จะทำไม่ได้ เว้นแต่มีคำสั่ง หมายของศาล หรือ มีเหตุตามที่กฎหมายบัญญัติ นั้นหมายความว่า กฎหมาย การกำหนดหลักเกณฑ์เกี่ยวกับการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันนั้นเป็นสิ่งที่จำเป็น โดยปัจจุบันการบัญญัติ ให้รัฐสามารถกระทำการดังกล่าวในระบบกฎหมายไทยนั้น กระจายอยู่ตามกฎหมายเฉพาะต่าง ๆ เช่น พระราชบัญญัติ การสอบสวนคดีพิเศษ พ.ศ. 2547 พระราชบัญญัติป้องกันและปราบปรามยาเสพติดให้โทษ พ.ศ. 2519 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เป็นต้น ซึ่งกฎหมายแต่ละฉบับก็มีการกำหนดหลักเกณฑ์บางประเด็น แตกต่างกัน และหลักเกณฑ์ที่กำหนดอยู่ในกฎหมายเฉพาะ ทั้งหลายก็ยิ่งขาดรายละเอียดบางประการ

ด้วยเหตุนี้ สถาบันพระปกเกล้า ในฐานะองค์กรที่มีหน้าที่ ส่งเสริมและสนับสนุนงานวิชาการแก่รัฐสภา จึงได้จัดทำโครงการ เรื่อง “กฎหมายเกี่ยวกับการกำหนดให้รัฐเข้าถึง หรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน : กรณีศึกษาต่างประเทศ” โดย นักวิชาการผู้มีความรู้ ความเชี่ยวชาญ ได้ดำเนินการศึกษา เปรียบเทียบประกอบไปด้วยกรณีศึกษา 5 เรื่อง ซึ่งเรื่องแรก เป็นการศึกษาเกี่ยวกับแนวคิดทฤษฎีที่เกี่ยวข้อง เพื่อศึกษา ในประเด็นการสร้างสมดุลระหว่างการคุ้มครองสิทธิส่วนบุคคล

และความมั่นคงของรัฐ ส่วนเรื่องที่ 2 – 5 เป็นกรณีศึกษากฎหมายของต่างประเทศที่มีการบัญญัติกฎหมายกลางในประเด็นดังกล่าว ได้แก่ สหรัฐอเมริกา สหราชอาณาจักร สาธารณรัฐฝรั่งเศส และสหพันธ์รัฐเยอรมนี ทั้งนี้ สถาบันฯ มีความยินดีเป็นอย่างยิ่งในการเผยแพร่ชุดกรณีศึกษาทั้ง 5 เรื่องนี้ เพื่อใช้เป็นข้อมูลประกอบในการยกร่าง หรือพิจารณาร่างกฎหมายที่กำหนดหลักเกณฑ์กลางเกี่ยวกับการกำหนดให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน อันเป็นกฎหมายที่จะต้องออกตามรัฐธรรมนูญและอาจมีขึ้นในอนาคต



(ศาสตราจารย์ วุฒิสาร ตันไชย)

เลขาธิการสถาบันพระปกเกล้า

สารบัญ

เรื่อง	หน้า
คำนำ	III
บทนำ	VII
ข้อความเบื้องต้น	1
1. ความคุ้มครองตามกฎหมายพื้นฐาน	4
2. เป้าหมายของคดีอาญา	9
3. บทบัญญัติของกฎหมายที่ให้อำนาจรัฐเข้าถึงและได้มาซึ่งข้อมูล ที่บุคคลสื่อสารถึงกัน	14
3.1 ความทั่วไป	15
3.2 การดักและบันทึกการสื่อสารโทรคมนาคม	17
3.2.1 เงื่อนไขในการใช้มาตรการ	17
3.2.2 ข้อมูลที่สามารถดักและบันทึกได้	21
3.2.3 ผู้มีอำนาจอนุมัติใช้มาตรการ	24
3.2.4 บุคคลผู้ได้รับผลกระทบจากการใช้มาตรการ	26
3.2.5 ข้อมูลที่เกี่ยวข้องกับแกนกลางของการใช้ชีวิตส่วนตัว	27
3.3 การได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ (Verkehrsdaten)	29
4. การใช้และการเก็บรักษาข้อมูลที่ได้จากการใช้มาตรการ	34
4.1 กรณีการดักและบันทึกการสื่อสารโทรคมนาคม	35
4.2 กรณีการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ	36

สารบัญ

เรื่อง	หน้า
5. ความรับผิดทางอาญาเกี่ยวกับการได้มาโดยมิชอบซึ่งข้อมูล ที่บุคคลสื่อสารถึงกัน	38
5.1 ความผิดฐานล่องล้าความเป็นส่วนตัวของคำพูด	39
5.2 ความผิดฐานล่องรู้ความลับในจดหมาย	42
6. หลักเกณฑ์การรับฟังข้อมูลที่บุคคลสื่อสารถึงกันเป็นพยานหลักฐาน	44
บรรณานุกรม	49



บทนำ

การคุ้มครองสิทธิส่วนบุคคล หรือที่ระบบกฎหมายประเทศเยอรมนีเรียกว่าสิทธิในความลับในการสื่อสารทางไกลนั้น เป็นสิทธิขั้นพื้นฐานที่ “กฎหมายพื้นฐาน” ซึ่งเป็นชื่อที่ประเทศเยอรมันใช้เรียกรัฐธรรมนูญนั้น คุ้มครองและคุ้มครองให้ กล่าวคือ กฎหมายพื้นฐานคุ้มครองความเป็นส่วนตัวของการสื่อสารกันระหว่างคู่สัญญาทั้งสองฝ่ายในฐานะที่สิทธิดังกล่าวนี้เป็นส่วนหนึ่งของสิทธิส่วนบุคคล อย่างไรก็ตาม ในบางกรณีกฎหมายก็ยอมให้รัฐสามารถจำกัดสิทธิดังกล่าวของบุคคลได้โดยกำหนดให้รัฐสามารถเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันได้ ในบางกรณี เช่นในกรณีที่มีความจำเป็นต้องแสวงหาพยานหลักฐานเพื่อประโยชน์ในการสืบสวนและสอบสวนคดีอาญา เป็นต้น

ในรายงานวิจัยฉบับนี้ ได้มีการศึกษาถึงกฎหมายในระบบกฎหมายของประเทศเยอรมันที่บัญญัติถึงการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน ซึ่งได้แก่ บทบัญญัติว่าด้วยการดักการสื่อสารโทรคมนาคม ซึ่งเป็นการบัญญัติเพื่อแก้ไขเพิ่มเติมเรื่องการให้รัฐเข้าถึงและได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกันในประมวลกฎหมายวิธีพิจารณาความอาญา โดยมีการกำหนดหลักเกณฑ์ในการขอเข้าถึงข้อมูลส่วนบุคคลว่า จะต้องเป็นกรณีที่ยอการเป็นผู้ร้องขออนุญาตต่อศาลเท่านั้น และถ้าหากศาลอนุมัติแล้ว ศาลก็จะออกหมายให้และผู้ให้บริการการสื่อสารโทรคมนาคมก็มีหน้าที่จะต้องเปิดช่องทางให้หน่วยงานของรัฐสามารถดักและบันทึกการสื่อสารได้ โดยมีการกำหนดเงื่อนไขในการขอยกหมายจากศาลว่า จะต้องเป็นกรณีที่ต้องปรากฏความสงสัยว่าจะมีการกระทำความผิดทางอาญาเกิดขึ้น และไม่ใช่ว่าความผิดทุกประเภทที่จะขอให้มีการดักฟังได้ แต่ต้องเป็นการกระทำความผิดที่เกี่ยวกับความมั่นคงของรัฐหรือเป็นกรณีความผิดอาญาอย่างร้ายแรง ที่สำคัญ จะต้องเป็นกรณีที่การแสวงหาพยานหลักฐานนั้นไม่สามารถทำได้ด้วยวิธีการอื่นแล้ว

นอกจากนี้ รายงานวิจัยฉบับดังกล่าวยังกล่าวถึงหลักเกณฑ์ของศาลในการรับฟังพยานหลักฐานที่ได้มาจากการดักฟังการสื่อสารของบุคคลด้วย โดยมีการศึกษาทฤษฎีที่นักกฎหมายเยอรมนีได้พยายามวางหลักไว้ที่สำคัญ ยังมีการกล่าวถึงประมวลกฎหมายประเทศเยอรมนีที่บัญญัติถึงการลอบฟังบุคคลที่ได้มาโดยมิชอบซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน ซึ่งเมื่อศึกษารายละเอียดแล้ว จะเห็นได้ว่า ระบบกฎหมายของประเทศเยอรมนีได้วางหลักเกณฑ์ไว้อย่างชัดเจนในกรณีที่รัฐจะเข้าถึงหรือได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน โดยกำหนดให้รัฐต้องใช้อำนาจนั้นอย่างจำกัด เนื่องจากเป็นการละเมิดสิทธิขั้นพื้นฐานที่กฎหมายพื้นฐานได้บัญญัติรับรองไว้



ในสังคมยุคใหม่ที่เต็มไปด้วยข้อมูล การสื่อสารโทรคมนาคม (Telekommunikation/ Telecommunication) ทำให้เกิดการแลกเปลี่ยนข่าวสารระหว่างบุคคลที่อยู่ห่างไกลกันโดยอาศัยเทคโนโลยีของการสื่อสารทางไกล เช่น การใช้คลื่นแม่เหล็กไฟฟ้าผ่านสายเคเบิล การใช้ระบบไร้สาย หรือการใช้คลื่นแสง ข่าวสารที่ส่งด้วยเทคโนโลยีของการสื่อสารทางไกล มักมีลักษณะอ่อนไหวกว่าการสื่อสารด้วยวิธีการทั่วไป กล่าวคือ การสื่อสารด้วยการพูดในชีวิตประจำวันย่อมจะได้รับความคุ้มครองตามลักษณะของสถานที่ที่ผู้สนทนาเลือก หรือการสื่อสารด้วยจดหมายก็ได้รับความคุ้มครองจากการล่วงรู้ข้อความในจดหมายโดยไม่ได้รับอนุญาตด้วยวิธีการใส่ซองปิดผนึก แต่ในการสื่อสารด้วยเทคโนโลยีการสื่อสารทางไกล ผู้สื่อสารกลับต้องยอมให้ผู้ให้บริการเข้าถึงข้อมูลการสื่อสารเหล่านั้นได้ ทั้งบุคคลที่สามก็ยังสามารถใช้เทคโนโลยีบางประการเพื่อล่วงรู้หรือเข้าถึงข้อมูลที่คู่สนทนาสื่อสารถึงกันได้ การสื่อสารด้วยเทคโนโลยีของการสื่อสารทางไกลนี้ช่วยทำให้การสื่อสารระหว่างผู้คนสะดวกยิ่งขึ้น ผ่านวิธีการที่หลากหลายมากขึ้น แต่ในขณะเดียวกัน ก็ก่อให้เกิดความเสี่ยงสูงขึ้นที่จะถูกดักฟังข้อความเหล่านั้นโดยปราศจากร่องรอยใดๆ ได้ การสื่อสารโทรคมนาคมที่ปราศจากการคุ้มครองย่อมจะก่อให้เกิดปัญหากับเศรษฐกิจของประเทศ ความลับทางการค้าต่างๆ จำเป็นต้องได้รับการคุ้มครองจากรัฐเพื่อมิให้คู่แข่งในหรือนอกประเทศล่วงรู้ รวมถึงความลับในทางวิชาชีพแพทย์หรือนายความด้วย การค้าขายในชีวิตประจำวัน ไม่ว่าจะเป็นการโอนเงินผ่านระบบ eBanking หรือการสั่งซื้อสินค้าทางโทรศัพท์ ก็ควรจะต้องมีการคุ้มครองความไว้นับถือใจด้วย นอกจากนั้น การคุ้มครองความไว้นับถือใจในการสื่อสารโทรคมนาคมที่ไม่เพียงพออาจกระทบกระเทือนต่อการพัฒนาตนเองเกี่ยวกับการสื่อสารในสังคมประชาธิปไตยอีกด้วย

ใครก็ตามที่รู้ว่าการสนทนาของตนเองอาจถูกดักฟังจากบุคคลที่สามได้ เสรีภาพในการพัฒนาตนเองของเขาจะถูกจำกัดลง สิ่งที่เขาประสงค์จะสื่อสาร จะไม่ถูกพูดออกไปอย่างเปิดเผย สถานการณ์เช่นนี้มิใช่จะก่อให้เกิดความเสียหายต่อโอกาสในการพัฒนาตนเองของปัจเจกบุคคลเท่านั้น แต่จะก่อให้เกิดความเสียหายต่อส่วนรวมด้วย¹

¹ BVerfG, EuGRZ 1995, 355.



1. ความคุ้มครองตามกฎหมายพื้นฐาน

สิทธิในความลับในการสื่อสารทางไกลเป็นสิทธิขั้นพื้นฐานที่ได้รับ การยอมรับตั้งแต่ในมาตรา 117 รัฐธรรมนูญแห่งอาณาจักรไวมาร์ ฉบับ 11 สิงหาคม ค.ศ. 1919² อย่างไรก็ตาม ความคุ้มครองตามมาตรา 117 นี้ มีอายุไม่ถึง 15 ปี ก็ถูกยกเลิกโดยพรรคนาซีด้วยการออกประกาศ ประธานาธิบดีแห่งอาณาจักรเพื่อคุ้มครองประชาชนและรัฐ (Verordnung des Reichspräsidenten zum Schutz von Volk und Staat) มาตรา 1 แห่งประกาศฉบับดังกล่าวบัญญัติให้ยกเลิกมาตรา 117 รัฐธรรมนูญแห่ง อาณาจักรไวมาร์ ดังนั้น การละเมิดหรือล่วงล้ำความลับในการส่งจดหมาย พัสดุ โทรเลข หรือการสนทนาทางไกลอื่นๆ จึงสามารถทำได้โดยชอบด้วย กฎหมาย³

มาตรการดักและบันทึกการสื่อสารโทรคมนาคมตาม มาตรา 100a ประมวลกฎหมายวิธีพิจารณาความอาญาเยอรมัน (Strafprozessordnung - StPO) เป็นการล่วงล้ำสิทธิในความลับในการส่งจดหมาย พัสดุ หรือ การสนทนาทางไกลอื่นๆ ที่มาตรา 10 กฎหมายพื้นฐาน (Grundgesetz - GG) รับรองและคุ้มครอง คุณธรรมทางกฎหมายที่มาตรา 10 คุ้มครอง คือ ความเป็นส่วนตัวของการสื่อสารกันระหว่างคู่สนทนาสองฝ่ายในฐานะที่เป็น ส่วนหนึ่งของสิทธิส่วนบุคคล โดยมุ่งคุ้มครองปัจเจกบุคคลจากการละเมิด สิทธิจากการกระทำของรัฐเป็นสำคัญ⁴ มาตรา 10 เป็นหลักประกัน

² Artikel 117 Weimarer Reichsverfassung vom 11. August 1919 "Das Briefgeheimnis sowie das Post-, Telegraphen- und Fernsprecheheimnis sind unverletzlich. Ausnahmen können nur durch Reichsgesetz zugelassen werden."

³ Neuhaus, FS-Rieß, 379.

⁴ BVerfGE 67, 152, 172; BVerfGE 85, 386, 396; BVerfGE 34, 238, 247; Grote, KritV 1999, 27, 38-39; Neuhaus, FS-Rieß, 375, 380-381.

การพัฒนาตนเองโดยเสรีในสังคมประชาธิปไตยด้วยการแลกเปลี่ยนข่าวสารความคิด หรือความคิดเห็นได้อย่างเป็นส่วนตัว การสนทนาที่เป็นส่วนตัวจะต้องเกิดขึ้นได้โดยปราศจากความกังวลว่าจะถูกบันทึกไว้หรือถูกนำไปใช้โดยปราศจากความยินยอมของคู่สนทนา เป็นการคุ้มครองการสื่อสารทางไกลที่เป็นส่วนตัวให้พ้นจากการใช้อำนาจของรัฐนั่นเอง⁵

สิ่งที่มาตรา 10 ให้การคุ้มครองเป็นประการแรกคือ เนื้อหาของการสื่อสารโทรคมนาคม⁶ โดยไม่ต้องคำนึงถึงว่าเนื้อหานั้นเป็นเนื้อหาที่คนธรรมดาสามารถเข้าใจได้ หรือเป็นเนื้อหาที่ผ่านขั้นตอนการเข้ารหัสไว้ จึงทำให้บุคคลธรรมดาไม่อาจเข้าใจได้ นอกจากนั้น สิทธิของผู้สื่อสารในการอนุญาตให้ใครล่วงรู้เนื้อหาของการสนทนา ก็เป็นสิ่งที่มาตรา 10 คุ้มครองเช่นเดียวกัน⁷ สิทธิในความลับในการสื่อสารทางไกลจึงรวมถึงสิทธิในการตัดสินใจของผู้สื่อสารในการที่จะคุ้มครองความลับของเขาด้วยวิธีการทางเทคนิคใดๆ ด้วย

นอกจากเนื้อหาของการสื่อสารโทรคมนาคมแล้ว สิทธิในความลับในการสื่อสารทางไกลยังคุ้มครองไปถึงรูปแบบและวิธีการในการสื่อสารด้วย ได้แก่ ข้อมูลเกี่ยวกับการเชื่อมต่อ ข้อมูลเกี่ยวกับตัวคู่สนทนา ระยะเวลาของการสนทนา ความถี่ของการสนทนา และสื่อที่ใช้ในการสนทนาด้วย ในกรณีของการใช้โทรศัพท์มือถือ ก็รวมถึงบริเวณและสถานที่ที่ผู้สนทนาอยู่ด้วย⁸

มาตรา 10 แห่งกฎหมายพื้นฐาน ก่อให้เกิดสิทธิเรียกร้องแก่ผู้ถูกระทบสิทธิในอันที่จะทราบถึงการใช้มาตรการดักการสื่อสารต่างๆ

⁵ BVerfGE 67, 157, 172.

⁶ BVerfGE 85, 386, 396.

⁷ BVerfGE 85, 386, 396; BVerfGE 67, 157, 172.

⁸ BVerfGE 85, 386, 396; BVerfGE 67, 157, 171.

ภายหลังจากที่การใช้มาตรการได้สิ้นสุดลงแล้ว เพื่อให้เขาสามารถตรวจสอบความชอบด้วยกฎหมายของการได้มาซึ่งเนื้อหาของการสนทนาและข้อมูลอื่นๆ และใช้สิทธิขอให้ลบข้อมูลเหล่านั้นได้⁹ มาตรา 10 บัญญัติว่า สิทธิในความลับในการสื่อสารทางไกลสามารถถูกล่วงละเมิดได้ด้วยบทบัญญัติของกฎหมาย โดยกฎหมายที่พุดถึงมาตรการที่อาจไปล่วงละเมิดสิทธิในความลับในการสื่อสารทางไกล จะต้องปรากฏบทบัญญัติที่แน่นอนและชัดเจนเกี่ยวกับวัตถุประสงค์ของมาตรการ เงื่อนไขในการใช้มาตรการ ขอบเขตและวิธีการใช้มาตรการเหล่านั้น และเมื่อมาตรการมีลักษณะรุนแรงมากขึ้น เงื่อนไขต่างๆ ก็ต้องเข้มข้นมากขึ้นเช่นกัน¹⁰

ฝ่ายนิติบัญญัติมองว่า มาตรการทางอาญาที่กระทำโดยลับเป็นมาตรการที่ละเมิดสิทธิขั้นพื้นฐานของผู้ที่เกี่ยวข้องอย่างร้ายแรง แต่กลับมีเงื่อนไขที่อ่อนกว่าการใช้มาตรการทางอาญาที่เปิดเผย ทั้งมาตรการทางอาญาหลายประการก็มีผลไปกระทบสิทธิของบุคคลจำนวนมาก เช่น การดักการสื่อสารโทรคมนาคมตามมาตรา 100a และการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 100g และเนื่องจากเป็นมาตรการทางอาญาที่กระทำโดยลับ จึงมีโอกาที่จะกระทบต่อแกนกลางของการใช้ชีวิตส่วนตัว (Kernbereich privater Lebensgestaltung/ Core Area of Private Living) ได้เพราะผู้กระทบสิทธิไม่รู้ถึงการใช้มาตรการนั้นด้วยเหตุนี้เอง ฝ่ายนิติบัญญัติจึงให้ความสำคัญกับการชั่งน้ำหนักระหว่างประโยชน์ส่วนรวมกับประโยชน์ส่วนบุคคลมากเป็นพิเศษในการบัญญัติกฎหมายเกี่ยวกับเรื่องนี้¹¹

เพื่อให้มาตรการบังคับทางอาญาถูกตรวจสอบจากองค์กรที่เป็นอิสระก่อนการใช้มาตรการ กฎหมายจึงได้กำหนดให้ศาลซึ่งเป็นองค์กรที่มีความ

⁹ BVerfGE 100, 313, 361.

¹⁰ BVerfGE 100, 313, 372.

¹¹ BT-Drs. 16/5846 S.23.

เป็นอิสระเป็นผู้อนุมัติ และเนื่องจากการพึ่งข้อโต้แย้งจากผู้ถูกระทบสิทธิ ไม่อาจเกิดขึ้นได้ในการใช้มาตรการเหล่านี้ กฎหมายจึงกำหนดให้มีการ แจกกลับไปยังผู้ถูกระทบสิทธิในภายหลัง และเปิดช่องทางให้ผู้ถูกระทบ สิทธิสามารถได้รับความคุ้มครองตามกฎหมายได้ ทั้งนี้เพื่อรักษาไว้ซึ่ง หลักพึ่งความทุกฝ่าย (มาตรา 103 กฎหมายพื้นฐาน) และหลักความคุ้มครอง โดยกฎหมายที่มีประสิทธิภาพ (มาตรา 19 กฎหมายพื้นฐาน) นอกจากนี้ กฎหมายยังบัญญัติให้ใช้มาตรการเช่นนั้นได้เฉพาะกับฐานความผิดอาญา บางฐานเท่านั้น¹²

เนื่องจากเทคโนโลยีสมัยใหม่ที่สามารถทำให้มนุษย์เข้าถึงข้อมูลต่างๆ ได้มากขึ้น มาตรการทางอาญาที่กระทำโดยลับจึงมักทำให้ได้มาซึ่งข้อมูล ต่างๆ มากมาย และการส่งต่อหรือใช้ข้อมูลนั้นก็เป็นการละเมิดสิทธิในการ กำหนดการใช้ข้อมูล (Informationelle Selbstbestimmung) ซึ่งก็เป็นการ ละเมิดสิทธิซ้ำอีก ดังนั้น กรณีจึงถือเป็นการกิจของรัฐในสร้างวิธีการ ทางกฎหมายเพื่อเป็นหลักประกันการใช้ข้อมูลนั้นตามวัตถุประสงค์ ที่กฎหมายบัญญัติไว้¹³

¹² BT-Drs. 16/5846 S.23.

¹³ BT-Drs. 16/5846 S.23.



2. เป้าหมายของคดีอาญา

นักกฎหมายเยอรมันอธิบายว่า คดีอาญามีเป้าหมายอยู่ด้วยกัน 3 ประการ คือ คำตัดสินถึงความรับผิดชอบทางอาญาของผู้ถูกกล่าวหาที่ (1) ยุติธรรมอันมีความจริงเป็นพื้นฐานรองรับ (Materielle Gerechtigkeit/ Material Justice) (2) เป็นไปตามหลักเกณฑ์ตามกฎหมายวิธีพิจารณาความอาญา (Prozedurale Gerechtigkeit/ Procedural Justice) (3) อันทำให้ความมั่นคงปลอดภัยตามกฎหมายเกิดขึ้นในสังคม (Rechtsfrieden/ Peace under the Law)¹⁴

อย่างไรก็ตาม น้อยครั้งที่เป้าหมายของคดีอาญาทั้งสามประการจะเกิดขึ้นได้พร้อมกันในคดีหนึ่ง ๆ เมื่อใดก็ตามที่ปรากฏความขัดแย้งกันของเป้าหมายทั้งสาม กฎหมายวิธีพิจารณาความอาญาจะทำหน้าที่ตัดสินว่า ในสถานการณ์นั้น เป้าหมายใดมีคุณค่าสูงกว่า

การค้นหา **ความจริง** เป็นเป้าหมายที่มักถูกมองว่ามีคุณค่าสูงสุด เพราะกฎหมายวิธีพิจารณาความอาญามีขึ้นเพื่อให้กฎหมายอาญาสารบัญญัติใช้บังคับได้ และการจะบังคับใช้กฎหมายอาญาได้ก็ต้องอาศัยความจริง เมื่อความจริงปรากฏ คำพิพากษาคดีอาญาก็จะยุติธรรม เพราะผู้กระทำความผิดได้รับโทษตามสัดส่วนความชั่วของเขา ตามหลักความชั่ว (Schuldprinzip/ Principle of Culpability) แต่การค้นหาความจริงจะกระทำโดยไม่มีขอบเขตไม่ได้เพราะความสามารถของมนุษย์ในการค้นหาความจริงมีอยู่อย่างจำกัด ในอดีต เราเคยเชื่อกันว่าโลกแบน แต่ตอนนี้เราคิดว่าโลกกลม วันหน้าอาจจะมีทฤษฎีใหม่มาหักล้างว่าโลกมีรูปร่างเหมือนไข่ก็ได้ การค้นหาความจริงจึงจะต้องถูกจำกัดโดย **หลักเกณฑ์ตามกฎหมายวิธีพิจารณาความอาญา** อันเป็นหลักเกณฑ์ที่มีขึ้นเพื่อคุ้มครองสิทธิและเสรีภาพของผู้ที่เกี่ยวข้องในคดี และจำกัดการใช้อำนาจขององค์กร

¹⁴ Roxin/Schünemann, § 1, Rn.3.

ของรัฐ กฎหมายวิธีพิจารณาความอาญาจึงห้ามศาลรับฟังพยานหลักฐานที่เกิดขึ้นหรือได้มาโดยมิชอบ แต่เมื่อใดก็ตามที่ความจริงอันจะได้จากพยานหลักฐานนั้นเป็นความจริงที่สำคัญ และหลักเกณฑ์ตามกฎหมายวิธีพิจารณาความอาญาที่ถูกฝ่าฝืนเป็นหลักเกณฑ์ที่สำคัญน้อยกว่ากฎหมายวิธีพิจารณาความอาญาก็จะอนุญาตให้ศาลรับฟังพยานหลักฐานนั้นได้เพื่อให้ได้มาซึ่งความจริงแท้

นอกจากนั้น การค้นหาความจริงโดยไม่มีที่สิ้นสุด กล่าวคือ แม้มีคำพิพากษาถึงที่สุดแล้วยังจะนำคดีเดิมขึ้นมาพิจารณาได้ใหม่หากสงสัยว่าคำพิพากษานั้นไม่สอดคล้องกับความจริง กฎหมายก็ไม่ยอมรับอีกเช่นกัน คำพิพากษาคดีอาญาจะต้องมีสภาพเด็ดขาดทางกฎหมายของคำพิพากษาอันจะทำให้เกิด **ความมั่นคงปลอดภัยตามกฎหมาย** ขึ้นในสังคม แม้ว่าคำพิพากษานั้นจะขัดแย้งกับความจริงก็ตาม สังคมที่ยอมรับให้มีการแก้ไขคำพิพากษาคดีอาญาได้โดยไม่มีที่สิ้นสุดจะเป็นสังคมที่ขาดความมั่นคงปลอดภัยตามกฎหมาย ผู้ถูกตัดสินไม่อาจใช้ชีวิตได้อย่างสงบเพราะจะต้องคอยนึกกังวลอยู่ตลอดเวลาว่าตนอาจถูกดำเนินคดีเพราะเรื่องเดิมอีกได้ อันจะทำให้สิทธิและเสรีภาพของเขาถูกระทบกระเทือนอย่างรุนแรงด้วยเหตุนี้เอง กฎหมายจึงอนุญาตให้การรื้อฟื้นคดีอาญาขึ้นพิจารณาใหม่กระทำได้ภายใต้เงื่อนไขที่จำกัดมาก

การศึกษาถึงเป้าหมายของคดีอาญา 3 ประการนี้ทำให้เข้าใจว่าข้อห้ามในกฎหมายพยานหลักฐานเป็นทางออกของกฎหมายวิธีพิจารณาความอาญาเมื่อการค้นหาความจริงเดินสวนทางกับการคุ้มครองสิทธิและเสรีภาพของผู้ถูกกล่าวหา นั่นเอง ข้อห้ามในกฎหมายพยานหลักฐานเป็นสิ่งที่มาจำกัดหน้าที่และความเป็นไปได้ในการค้นหาความจริงในคดีอาญาเพื่อคุ้มครองประโยชน์อื่นที่กฎหมายเห็นว่าสำคัญกว่าประโยชน์ส่วนรวมอันเกิดจากการดำเนินคดีอาญา ประโยชน์ที่ว่านั้นก็คือ สิทธิขั้นพื้นฐานของปัจเจกบุคคล (Grundrechte der Einzelpersonlichkeit/ Individual

Rights) นั่นเอง¹⁵ ข้อห้ามการนำสืบพยานหลักฐานจึงมิใช่สิ่งอื่นใด หากแต่เป็นเครื่องมืออย่างหนึ่งในการคุ้มครองสิทธิขั้นพื้นฐานและสิทธิส่วนบุคคล¹⁶ เหมือนที่ศาลรัฐธรรมนูญแห่งสหพันธ์ (Bundesverfassungsgericht - BVerfG) ได้เคยอธิบายว่า แม้ว่าคดีอาญาจะมีเป้าหมายในการค้นหาความจริง แต่การค้นหาความจริงจะทำโดยไร้ขอบเขตไม่ได้¹⁷ กฎหมายเรียกร้องให้มีการคุ้มครองคุณค่าและสิทธิอื่นในคดีอาญาด้วย เช่น สิทธิส่วนบุคคลของผู้ที่มีส่วนเกี่ยวข้องในคดี และในขณะเดียวกัน ก็เรียกร้องให้กระบวนการยุติธรรมทางอาญาดำเนินไปอย่างมีประสิทธิภาพ มิเช่นนั้น ความเป็นนิติรัฐคงจะไม่เกิดขึ้นอย่างสมบูรณ์¹⁸ หากฝ่ายนิติบัญญัติมุ่งแต่คุ้มครองสิทธิส่วนบุคคลจนเกินสัดส่วน โดยบัญญัติข้อห้ามในกฎหมายพยานหลักฐานเอาไว้มากมาย จนทำให้พยานหลักฐานที่มีอยู่ไม่อาจเข้าสู่การรับรู้ของศาลได้ ฝ่ายนิติบัญญัติก็ต้องเผชิญหน้ากับความบกพร่องของกระบวนการยุติธรรม ข้อจำกัดการค้นหาความจริงของศาลที่เกิดจากข้อห้ามในกฎหมายพยานหลักฐานจะส่งผลให้เกิดภาวะแก่กระบวนการยุติธรรมในการสร้างความสงบเรียบร้อยในสังคม และในที่สุด ก็จะก่อให้เกิดอันตรายต่อคุณธรรมทางกฎหมายที่กฎหมายประสงค์จะคุ้มครอง อย่างไรก็ตาม จะด่วนสรุปว่าข้อห้ามในกฎหมายพยานหลักฐานไม่ใช่สิ่งที่รัฐธรรมนูญพึงปรารถนา ก็คงจะไม่ถูกต้องนัก ทั้งนี้เพราะหลักนิติรัฐไม่เคยเรียกร้องให้มีการค้นหาความจริงโดยปราศจากขอบเขต เพื่อรักษาไว้ซึ่งคุณค่าที่สำคัญกว่า การยอมรับข้อจำกัดของการค้นหาความจริงจึงเป็นเรื่องที่เกิดขึ้นได้ ซึ่งเป็นกรณีที่ประโยชน์ส่วนรวมอันจะเกิดจากกระบวนการยุติธรรมที่มีประสิทธิภาพมีน้ำหนักน้อยกว่าประโยชน์ส่วนบุคคลที่จะเกิด

¹⁵ Henkel, 271; Rogall, ZStW 1979, 1, 8.

¹⁶ Rogall, ZStW 1979, 1, 9.

¹⁷ โปรดดู BGHSt 14, 358, 365; 17, 337, 348.

¹⁸ BVerfGE 33, 367, 383; 38, 105, 115f.; 38, 312, 321; 39, 156, 163; 41, 246, 250; 44, 353, 374.

จากการจำกัดการรับรู้พยานหลักฐานของศาล เมื่อใดที่คุณค่าประการใดจะมีความสำคัญมากกว่ากัน เราไม่สามารถตอบได้ในลักษณะที่เป็นหลักการทั่วไป แต่ศาลจะเป็นผู้ชี้แจงน้ำหนักคุณค่าสองประการนี้เมื่อมีกรณีปัญหาเกิดขึ้นเป็นกรณีๆ ไป¹⁹ บทบัญญัติที่เป็นข้อห้ามการนำสืบพยานหลักฐานในกฎหมายปัจจุบันเป็นผลลัพธ์ของการชี้แจงน้ำหนักโดยฝ่ายนิติบัญญัติระหว่างประโยชน์ส่วนรวมที่จะเกิดจากกระบวนการยุติธรรมที่มีประสิทธิภาพกับประโยชน์ส่วนบุคคลที่ถูกล่วงละเมิด ข้อห้ามในกฎหมายพยานหลักฐานจึงถือเป็นบทบัญญัติที่เกี่ยวข้องกับกฎหมายรัฐธรรมนูญโดยตรง²⁰

¹⁹ BVerfGE 33, 367 ff.; BVerfGE 38, 312 ff; BVerfG, NJW 1977, 1490 ff.

²⁰ Rogall, ZStW 1979, 1, 4, 10.



3. บทบัญญัติของกฎหมายก็ให้อำนาจรัฐเข้าถึง และได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน

ในหัวข้อนี้ จะได้กล่าวถึงบทบัญญัติของกฎหมายที่ให้อำนาจรัฐเข้าถึง และได้มาซึ่งข้อมูลที่บุคคลสื่อสารถึงกัน โดยจะได้กล่าวถึงความทั่วไปในเรื่องนี้เสียก่อน แล้วก็จะได้กล่าวถึงการดักและบันทึกการสื่อสารโทรคมนาคม และการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ โดยมีรายละเอียดดังนี้

3.1 ความทั่วไป

บทบัญญัติว่าด้วยการดักการสื่อสารโทรคมนาคม (Überwachung der Telekommunikation/Telecommunication Surveillance) ถูกบัญญัติขึ้นครั้งแรกโดยกฎหมายว่าด้วยการจำกัดสิทธิในความลับในการส่งจดหมายพัสดุ และการติดต่อทางไกลอื่น (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses – Artikel 10-Gesetz - G10) เมื่อปี ค.ศ. 1968 อันเป็นช่วงเวลาที่มีความไม่แน่นอนทางการเมืองเกิดขึ้นในเยอรมนีตะวันตก²¹ มาตรา 2 แห่งกฎหมายฉบับนี้บัญญัติให้มีการเพิ่มเติมมาตรา 100a และมาตรา 100b เข้ามาในประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งให้อำนาจเจ้าพนักงานของรัฐในการแอบฟังและแอบอ่านการสื่อสารทางไกลระหว่างกันของบุคคล ก่อนหน้านี้นี้ หน่วยงานของรัฐมีอำนาจเพียงร้องขอข้อมูลจากหน่วยงานอื่น และร้องขอได้แต่เพียงข้อมูลเกี่ยวกับการเชื่อมต่อ (Call Detail Record - CDR) ของการสื่อสารทางไกลเท่านั้น²² รวมถึงให้อำนาจค้นและยึดจดหมายตามมาตรา 99 ประมวลกฎหมายวิธีพิจารณาความอาญา ซึ่งทำให้ได้มาซึ่งข้อมูลเกี่ยวกับพฤติกรรมของผู้ถูกกล่าวหาในการติดต่อสื่อสารกัน การตรากฎหมายที่ให้อำนาจหน่วยงานของรัฐในการดักการสื่อสารโทรคมนาคมนี้เป็นผลผลิต

²¹ Hauck, 7. Kapitel, §5, S.359-360.

²² Neuhaus, FS-Rieß, 3380.

ข้างเคียงของบทบัญญัติว่าด้วยอำนาจของหน่วยสืบราชการลับในการดัก การสื่อสารโทรคมนาคม การประกาศใช้กฎหมาย G 10 นี้มีผลทำให้ กฎหมายที่ให้อำนาจฝ่ายสัมพันธ์มิตรควบคุมการสื่อสารภายในประเทศ เยอรมนีตะวันตกได้ถูกยกเลิกไป

ตั้งแต่ปี ค.ศ. 1968 เป็นต้นมา บทบัญญัติมาตรา 100a และ มาตรา 100b ถูกแก้ไขเปลี่ยนแปลงหลายครั้ง ในช่วงปี 70 เป็นการแก้ไข เพิ่มเติมเพื่อต่อสู้กับผู้ก่อการร้าย และอีกครั้งหนึ่งในช่วงปี 90 ที่มีการ เพิ่มเติมมาตรการบังคับทางอาญา โดยเฉพาะมาตรการบังคับทางอาญา ที่กระทำโดยลับ อย่างไรก็ตาม อาจกล่าวโดยสรุปได้ว่า การแก้ไขเพิ่มเติม ส่วนมากเป็นการแก้ไขเพิ่มเติมเพื่อเพิ่มฐานความผิดที่ให้เจ้าพนักงาน สามารถดักการสื่อสารโทรคมนาคมได้ การแก้ไขครั้งล่าสุดเกิดขึ้นเมื่อ เดือนกันยายน พ.ศ. 2560 ด้วยกฎหมายว่าด้วยการจัดการคดีอาญาให้มี ประสิทธิภาพและเหมาะสมกับทางปฏิบัติ (*Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens*) เป็นการแก้ไข เพิ่มบทบัญญัติที่ให้อำนาจแก่หน่วยงานของรัฐในการดักและบันทึก การสื่อสารโทรคมนาคมที่เข้ารหัสไว้และค้นออนไลน์ได้เป็นครั้งแรก

การให้อำนาจแก่หน่วยงานของรัฐในการดักฟังการสื่อสารทาง โทรคมนาคมเพื่อประโยชน์ในการดำเนินคดีอาญานั้น เป็นความพยายาม จากทั้งฝ่ายการเมือง ฝ่ายตุลา และฝ่ายปฏิบัติ จึงได้รับการยอมรับจาก ทุกฝ่ายโดยรวดเร็ว ด้วยเหตุผลว่ามาตรการนี้เป็นมาตรการที่จำเป็น เพื่อดำเนินคดีอาญากับอาชญากรรมรูปแบบใหม่ๆ โดยเฉพาะอย่างยิ่ง อาชญากรรมที่กระทำโดยองค์กรอาชญากรรม²³ ข้อวิพากษ์วิจารณ์ที่ปรากฏ จึงมักมิได้มุ่งเป้าไปที่การมีอยู่ของมาตรการ แต่พุ่งเป้าไปที่จำนวนครั้งที่มีการใช้มาตรการนี้ที่เพิ่มมากขึ้นมากในแต่ละปี²⁴ ขอบเขตที่กว้างขวาง

²³ Rudolphi, ZRP 1976, 165, 167.

²⁴ โปรตุเกส Albrecht/Dorsch/Krüpe-Gescher, S.27 ff.

ของฐานความผิดที่กฎหมายอนุญาตให้ดักการสื่อสารโทรคมนาคมได้ การควบคุมการใช้มาตรการโดยศาล และผลกระทบที่บุคคลที่สามอาจได้รับจากการใช้มาตรการ²⁵

3.2 การดักและบันทึกการสื่อสารโทรคมนาคม

ในหัวข้อนี้ จะได้กล่าวถึงมาตรการดักและบันทึกการสื่อสารโทรคมนาคม โดยจะได้กล่าวถึงเงื่อนไขในการใช้มาตรการเป็นลำดับแรก และจะกล่าวถึงข้อมูลที่สามารถดักและบันทึกได้ ผู้มีอำนาจอนุมัติให้ใช้มาตรการ บุคคลผู้ได้รับผลกระทบจากการใช้มาตรการ ข้อมูลที่เกี่ยวข้องกับแกนกลางของการใช้ชีวิตส่วนตัว และการตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการ ปรากฏรายละเอียดดังนี้

3.2.1 เงื่อนไขในการใช้มาตรการ

1) ต้องปรากฏความสงสัยว่ามีการกระทำความผิดอาญาเกิดขึ้น

มาตรา 100a วรรคแรก ประมวลกฎหมายวิธีพิจารณาความอาญา ได้บัญญัติถึงเงื่อนไขในการใช้มาตรการดักและบันทึกการสื่อสารโทรคมนาคมว่า จะต้องปรากฏข้อเท็จจริงที่สนับสนุนว่ามีความสงสัยว่าการกระทำความผิดอาญาที่บัญญัติไว้ในมาตรา 100a เกิดขึ้นเสียก่อน ความสงสัยที่มาตรา 100a ต้องการนี้เป็นเพียงความสงสัยระดับเบื้องต้น (Anfangsverdacht) เท่านั้น²⁶ ซึ่งโดยปกติ เป็นความสงสัยในระดับที่ประมวลกฎหมายวิธีพิจารณาความอาญานำบัญญัติให้เจ้าพนักงานเริ่มทำการสอบสวนคดีอาญาเท่านั้น²⁷ ในการวินิจฉัยว่าความสงสัยระดับ

²⁵ Albrecht/Dorsch/Krüpe-Gescher, S.10; Krüpe-Gescher, S.20.

²⁶ BGBSt 41, 33; Albrecht/Dorsch/Krüpe-Gescher, S.11; Kindhäuser, StPO, § 8, Rn.76; Meyer-Gossner/Schmitt, § 100a, Rn.6; Roxin/Schünemann, § 36, Rn.3.

²⁷ § 152 II StPO

เบื้องต้นปรากฏขึ้นหรือไม่ เป็นดุลพินิจของศาลซึ่งเป็นผู้มีอำนาจออกหมาย
ดักการสื่อสารโทรคมนาคม²⁸

มีนักวิชาการวิพากษ์วิจารณ์ว่า ความสงสัยระดับ
เบื้องต้นอาจเป็นความสงสัยที่เบาบางเกินกว่าที่จะมาใช้เป็นเงื่อนไขในการใช้
มาตรการดักการสื่อสารโทรคมนาคม นอกจากนั้น ข้อวิพากษ์วิจารณ์
ยังพุ่งเป้าไปถึงประเด็นที่ว่า ศาลมีดุลพินิจกว้างขวางมากในการพิจารณาว่า
ปรากฏความสงสัยระดับเบื้องต้นว่ามีความผิดอาญาเกิดขึ้นหรือไม่
การควบคุมการใช้อำนาจของเจ้าพนักงานโดยฝ่ายศาลจึงไม่มีประสิทธิภาพ
ตามที่บทบัญญัติของกฎหมายคาดหวังเอาไว้²⁹

2) ฐานความผิดที่สามารถใช้มาตรการได้

การดักการสื่อสารโทรคมนาคมนี้ ไม่สามารถทำได้ใน
การสอบสวนคดีอาญาทุกฐานความผิด แต่จะต้องเป็นฐานความผิดที่ปรากฏ
ในมาตรา 100a วรรคสองเท่านั้น ทั้งนี้เพราะการดักฟังการสื่อสาร
โทรคมนาคมในการสอบสวนคดีอาญาทุกฐานความผิดจะเป็นการละเมิดต่อ
สิทธิขั้นพื้นฐานอย่างรุนแรง ทั้งบุคคลที่สามที่ไม่เกี่ยวข้องก็อาจได้รับ
ผลกระทบได้ เมื่อครั้งที่ได้มีการนำเอามาตรการดักการสื่อสารโทรคมนาคม
มาใช้เป็นครั้งแรก ผู้ร่างกฎหมายกำลังกังวลเรื่องศัตรูของรัฐและอาชญากร
ร้ายแรงที่อาจได้รับความคุ้มครองจากสิทธิในความลับในการติดต่อสื่อสาร
ทางไกล³⁰ ฐานความผิดที่สามารถใช้มาตรการดักการสื่อสารโทรคมนาคม
ได้จึงล้วนเป็นความผิดเกี่ยวกับความมั่นคงของรัฐและความผิดอาญา
ร้ายแรง อย่างไรก็ตาม ตลอด 50 ปีของการใช้บังคับมาตรา 100a มีการ
แก้ไขเพิ่มเติมมาตรานี้ทั้งสิ้นถึง 25 ครั้ง และส่วนมาก เป็นการแก้ไข

²⁸ BGHSt 41, 33.

²⁹ Küpper, JR 1996, 214; Störmer, StV 1995, 653, 655; Bernsmann, NStZ 1995, 512, 513.

³⁰ Neuhaus, FS-Rieß, 381.

เพิ่มเติมเพื่อเพิ่มเติมฐานความผิดที่อาจถูกดักการสื่อสารโทรคมนาคมได้ จนเป็นที่วิพากษ์วิจารณ์อย่างกว้างขวาง³¹

เนื่องจากการแอบดักการสื่อสารโทรคมนาคมเป็น มาตรการบังคับทางอาญาที่จะเมิดต่อสิทธิและเสรีภาพที่กฎหมายรองรับ อย่างมาก การใช้มาตรการจึงควรทำได้ในกรณีความผิดอาญาที่มีความไม่ ชอบธรรม (Unrecht/ Wrongdoing) มากเป็นกรณีพิเศษ และเป็นกรณี ที่กฎหมายอนุญาตให้ทำได้เป็นกรณีพิเศษเท่านั้น อย่างไรก็ตาม หากพิจารณา บรรดาฐานความผิดที่ระบุไว้ในมาตรา 100a แล้วจะพบว่า บทบัญญัติ ดังกล่าวมิได้เดินตามแนวทางที่กล่าวมาแต่อย่างใด ตรงกันข้าม กลับแสดง ให้เห็นว่าฝ่ายนิติบัญญัติเลือกฐานความผิดตามอำเภอใจ และตามนโยบาย ทางอาญาที่เป็นประเด็นทางการเมืองในขณะนั้น ๆ³² โดยเฉพาะอย่างยิ่ง การนำเอาความผิดอาญาประเภทก่ออันตรายเชิงนามธรรม (abstrakte Gefährdungsdelikt) ความผิดอาญาที่มีโทษจำคุกขั้นต่ำไม่ถึง 1 ปี และ ความผิดอาญาที่กระทำโดยประมาท เข้ามาบรรจุอยู่ในฐานความผิดที่ สามารถใช้มาตรการดักการสื่อสารโทรคมนาคมได้ เพราะความผิดเหล่านี้ ไม่ใช่ความผิดอาญาร้ายแรงตามเจตนารมณ์ดั้งเดิมของผู้ร่างกฎหมาย แต่อย่างใด³³

นอกจากนั้น การเพิ่มเติมความผิดเกี่ยวกับอาวุธ ความผิดเกี่ยวกับยาเสพติด และความผิดเกี่ยวกับทรัพย์สินก็ถูกวิพากษ์วิจารณ์ เป็นอย่างมากว่าขัดแย้งกับเจตนารมณ์ดั้งเดิมของมาตรา 100a ฝ่าย นิติบัญญัติเอง เมื่อครั้งที่มีการเพิ่มเติมความผิดเกี่ยวกับอาวุธและความผิด เกี่ยวกับยาเสพติดเข้ามา ก็ให้เหตุผลว่าความผิดประเภทนี้เป็นความผิด ที่เกี่ยวข้องกับการสื่อสาร³⁴ กล่าวคือ ไม่มีสิ่งใดเกี่ยวข้องกับความผิดอาญา

³¹ Welp, Mangakis-FS, 813 f.

³² Albrecht/Dorsch/Krüpe-Gescher, S.6; Niehaus, S.40 f.; Welp, S.65

³³ Neuhaus, S.386 f.; Niehaus, S.91 f.

³⁴ BT-Drs. VI/2722 S.4.

ร้ายแรงหรือความผิดเกี่ยวกับความมั่นคงของรัฐเลย ทั้งในบรรดาความผิดเกี่ยวกับยาเสพติดที่บรรจุไว้ในมาตรา 100a นั้น มีบางฐานความผิดที่เป็นการใช้ยาเสพติด ซึ่งก็ขัดแย้งกับที่ฝ่ายนิติบัญญัติได้เคยกล่าวไว้ในเอกสารประกอบการแก้ไขเพิ่มเติมมาตรา 100a ว่าจะจำกัดเฉพาะเพียงความผิดเกี่ยวกับการค้ายาเสพติดและความผิดยาเสพติดที่กระทำโดยองค์กรการค้ายาเสพติดเท่านั้น³⁵

3) การแสวงหาพยานหลักฐานไม่อาจทำได้ด้วยวิธีการอื่น

มาตรา 100a บัญญัติให้หน่วยงานของรัฐสามารถใช้มาตรการดักการสื่อสารโทรคมนาคมนี้ได้ก็ต่อเมื่อการค้นหาคำความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือแทบจะเป็นไปไม่ได้เลย หลัก Subsidiarity นี้แสดงให้เห็นถึงความพยายามของฝ่ายนิติบัญญัติในการรักษาไว้ซึ่งความได้สัดส่วนระหว่างสิทธิในความลับในการสื่อสารทางไกลกับการใช้อำนาจดักการสื่อสารโทรคมนาคม กล่าวได้อีกอย่างหนึ่งว่า ฝ่ายนิติบัญญัติพยายามให้มีการใช้มาตรการดักการสื่อสารโทรคมนาคมได้เฉพาะในกรณีที่มาตรการบังคับทางอาญาอื่นๆ ไปจะล้มเหลวหรืออาจจะล้มเหลวเท่านั้น³⁶ ในคำร้องขอใช้มาตรการดักการสื่อสารโทรคมนาคม จึงจะต้องมีข้อความชี้แจงไว้ด้วยว่า การสอบสวนโดยไม่ใช่มาตรการดังกล่าวไม่อาจประสบความสำเร็จได้หรืออาจทำได้โดยยากลำบากอย่างไร และเพราะเหตุใด

ศาลสูงสุดแห่งสหพันธ์เคยวินิจฉัยไว้ในคดี BGHSt 41, 33 ff. ว่ากรณีใดจะถือว่าเป็นกรณีที่มีการค้นหาคำความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือ

³⁵ Niehaus, S.57 f.

³⁶ Albrecht/Dorsch/Krüpe-Gescher, S.20.

แทบจะเป็นไปไม่ได้เลย เป็นกรณีที่กฎหมายให้เป็นดุลพินิจของศาลเพราะกฎหมายเลือกใช้ถ้อยคำที่มีความหมายกว้าง คำพิพากษานี้ถูกวิพากษ์วิจารณ์จากฝ่ายวิชาการว่า การปล่อยให้การวินิจฉัยว่ากรณีใดเป็นกรณีที่ต้องการค้นหาความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือแทบจะเป็นไปไม่ได้เลย ตกเป็นเรื่องของดุลพินิจของศาล จะส่งผลให้กลไกควบคุมการใช้มาตรการที่กฎหมายสร้างไว้ไม่อาจสำเร็จได้ การที่กฎหมายเลือกใช้ถ้อยคำกว้างๆ นี้เป็นช่องทางในการสร้างและพัฒนาหลักกฎหมายเพื่อควบคุมการใช้มาตรการให้ชัดเจนและเป็นระบบ³⁷

3.2.2 ข้อมูลซึ่งสามารถดักและบันทึกได้

ในการแก้ไขเพิ่มเติมมาตรา 100a และ 100b ประมวลกฎหมายวิธีพิจารณาความอาญา เมื่อปี ค.ศ. 1997³⁸ ได้มีการยกเลิกการใช้คำว่า “การสื่อสารทางไกล” (Fernmeldeverkehr) และเปลี่ยนมาใช้คำว่า “การสื่อสารโทรคมนาคม” (Telecommunication) แทน หมายความว่าถึงขั้นตอนทางเทคนิคในการส่ง ถ่ายทอด และรับสัญญาณด้วยอุปกรณ์การสื่อสารทางไกล ซึ่งเป็นความหมายเดียวกันกับมาตรา 3 อนุมาตรา 22 กฎหมายว่าด้วยการสื่อสารทางไกล (Telekommunikationsgesetz - TKG) โดยอาศัยมาตรานี้ รัฐสามารถได้มาซึ่งเนื้อหาของการสื่อสารโทรคมนาคมและบันทึกเนื้อหาของการสื่อสารนั้นที่กำลังเดินทางจากผู้สื่อสารคนหนึ่งไปยังผู้สื่อสารอีกคนหนึ่งในเครือข่ายโทรคมนาคมสาธารณะ³⁹ ความหมายนี้ครอบคลุมถึงการส่งข้อความผ่านกระบวนการสื่อสารทางไกลทุกรูปแบบ

³⁷ Küpper, JR 1996, 214; Bernsmann, NSTZ 1995, 512, 513.

³⁸ Begleitgesetz zum Telekommunikationsgesetz vom 17.12.1997, BGBl I 3108, S.3113.

³⁹ BT-Drs. 18/12785 S.48.

ไม่ว่าจะเป็นในรูปแบบของสัญลักษณ์ ภาษา หรือเสียง⁴⁰ ซึ่งได้แก่ การสื่อสารด้วยโทรศัพท์บ้าน โทรศัพท์เคลื่อนที่ การส่งข้อความผ่านบริการส่งข้อความสั้น (SMS) และข้อความมัลติมีเดีย (MMS) รวมถึงการส่งโทรสารและโทรพิมพ์⁴¹ การดักการสื่อสารโทรคมนาคมตามมาตรา 100a ประมวลกฎหมายวิธีพิจารณาความอาญา จะต้องเป็นดักการสื่อสารโทรคมนาคมที่กำลังดำเนินอยู่เท่านั้น หากการสื่อสารโทรคมนาคมสิ้นสุดลงแล้ว เจ้าพนักงานจะใช้มาตรา 100a ไปดักมาไม่ได้⁴² นอกจากนี้ การจะเป็นการสื่อสารโทรคมนาคมได้จะต้องปรากฏผู้สื่อสารที่เป็นมนุษย์อย่างน้อย 1 คน การส่งข้อมูลจากเครื่องมือหรืออุปกรณ์ใดไปยังเครื่องมือหรืออุปกรณ์อีกอันหนึ่งโดยอัตโนมัติ จึงไม่ใช่การสื่อสาร ดังนั้น ข้อมูลเกี่ยวกับสถานที่อยู่ของโทรศัพท์มือถือที่ถูกส่งจากโทรศัพท์มือถือไปยังศูนย์กลางข้อมูลโดยอัตโนมัติ จึงไม่อาจใช้มาตรการตามมาตรา 100a ไปเอามาได้⁴³ การติดตามตำแหน่งของโทรศัพท์มือถือโดยการใช้อุปกรณ์ IMSI-Catcher ก็เพิ่งสามารถทำได้เมื่อมีการเพิ่มเติมมาตรา 100i เข้ามาในประมวลกฎหมายวิธีพิจารณาความอาญาเมื่อปี ค.ศ. 2002

อย่างไรก็ตาม ในปัจจุบันอินเทอร์เน็ตเข้ามามีบทบาทสำคัญในชีวิตประจำวัน และเครื่องมือและอุปกรณ์ต่างๆ ก็ถูกพัฒนาให้เหมาะสมกับการใช้งานมากยิ่งขึ้น การสื่อสารระหว่างกันของบุคคลจึงเกิดขึ้นบนอินเทอร์เน็ตมากขึ้น เช่น การโทรศัพท์ผ่านอินเทอร์เน็ต (Voice-over-IP - VoIP) หรือการส่งข้อความโดยใช้โปรแกรม messenger ต่าง ๆ

⁴⁰ Kindhäuser, StPO, § 8, Rn.75; Roxin/Schünemann, § 36, Rn.3.

⁴¹ Bundesministerium der Justiz und für Verbraucherschutz (BMJV), Bericht der Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens, (Berlin: BMJV, 2005), S.73.

⁴² Meyer-Gossner/Schmitt, § 100b, Rn.3; Vassilaki, JR 2000, 446, 447.

⁴³ Roxin/Schünemann, § 36, Rn.4; Vassilaki, JR 2000, 446, 447.

เป็นต้น เนื้อหาของการสื่อสารกันด้วยวิธีการเหล่านี้จะถูกเข้ารหัสเอาไว้ หน่วยงานที่มีอำนาจสอบสวนคดีอาญาจึงจะได้รับแต่เพียงข้อมูลที่ถูกเข้ารหัสเอาไว้ และการถอดรหัสก็ยังไม่สามารถกระทำได้โดยใช้เทคโนโลยีในปัจจุบัน หรือหากทำได้ก็ใช้เวลามากและมีค่าใช้จ่ายสูง การจะกำหนดให้เป็นหน้าที่ของผู้ให้บริการในการแจกจ่ายโปรแกรมถอดรหัสชั่วคราวที่สร้างขึ้นด้วยวิธีการอัตโนมัติให้แก่หน่วยงานของรัฐก็ยังไม่อาจเป็นไปได้ ดังนั้น เพื่อให้มาตรการในการสอบสวนคดีอาญามีความทันสมัยทัดเทียมกับความก้าวหน้าในด้านเทคโนโลยี และเพื่อการดำเนินคดีอาญาเป็นไปอย่างมีประสิทธิภาพ จึงได้มีการแก้ไขมาตรา 100a ประมวลกฎหมายวิธีพิจารณาความอาญา เปิดช่องทางให้หน่วยงานของรัฐสามารถได้มาซึ่งเนื้อหาของการสื่อสารด้วยวิธีการเหล่านี้ด้วย กล่าวคือ เนื้อหาก่อนที่จะเข้ารหัสหรือเนื้อหาหลังจากถอดรหัสแล้ว โดยใช้โปรแกรมพิเศษที่นำไปติดตั้งไว้ที่เครื่องมือหรืออุปกรณ์ปลายทางแล้ว (Quelle-TKÜ)⁴⁴

ในวรรคแรกแห่งมาตรา 100a จึงได้บัญญัติว่า หากจำเป็นเพื่อทำให้การดักและบันทึกการสื่อสารโทรคมนาคมที่อยู่ในรูปแบบที่เข้ารหัสไว้สามารถเกิดขึ้นได้ การดักฟังและการบันทึกการสื่อสารโทรคมนาคมสามารถกระทำได้โดยอาศัยวิธีการทางเทคนิคที่อาจเข้าไปรบกวนระบบเทคโนโลยีสารสนเทศของผู้ถูกละเมิดสิทธิได้ อาทิ การใช้สัญญาณเสียง เนื้อหาและข้อมูลอื่นๆ ที่ถูกเข้ารหัสไว้ที่จะถูกดักและบันทึกนี้ จะต้องเป็นเนื้อหาและข้อมูลที่สามารถถูกดักและบันทึกได้ด้วยวิธีการดักและบันทึกข้อมูลที่อยู่ในระหว่างการเดินทางเท่านั้น พุทธอีกอย่างหนึ่งว่าการดักและบันทึกการสื่อสารโทรคมนาคมที่มีการเข้ารหัสสามารถทำได้ เฉพาะเท่าที่การดักและบันทึกการสื่อสารทางไกลทำได้เท่านั้น บทบัญญัตินี้จึงเป็นการจำกัดขอบเขตของการใช้มาตรการดักการสื่อสารโทรคมนาคมไว้แต่เพียงเนื้อหาของการสื่อสารเท่านั้น แต่ไม่รวมถึงข้อมูลอื่นๆ ที่อยู่ใน

⁴⁴ BT-Drs. 18/12785 S.48-49.

ระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง⁴⁵ โปรแกรมที่จะนำมาใช้เพื่อคัดและบันทึกการสื่อสารโทรคมนาคมก็จะต้องสามารถตั้งค่าเพื่อให้ได้มาเฉพาะเพียงเนื้อหาของการสื่อสารตามที่กฎหมายกำหนดเท่านั้น ตรวจจับได้ตามที่โปรแกรมดังกล่าวยังไม่สามารถหามาได้ ซึ่งอาจเป็นเพราะยังไม่สามารถพัฒนาโปรแกรมได้ตามที่กฎหมายกำหนด การคัดและบันทึกการสื่อสารโทรคมนาคมยังไม่สามารถกระทำได้อีกครั้งในกระบวนการยุติธรรมจะต้องหามาตรการทางเทคนิคเพื่อให้มีการล้วงล้ำเข้าไปในระบบเทคโนโลยีสารสนเทศน้อยที่สุดและเพื่อคุ้มครองความมั่นคงปลอดภัยของข้อมูล ทั้งนี้ตามมาตรา 100a วรรคห้า

ในการคัดและบันทึกการสื่อสารโทรคมนาคมทางไกลและการคัดและบันทึกการสื่อสารโทรคมนาคมที่อุปกรณ์ต้นทางหรือปลายทาง (Quelle-TKÜ) จะสามารถทำได้กับเนื้อหาของการสื่อสารฯ ที่เกิดขึ้นหลังจากที่ศาลได้ออกหมายแล้วเท่านั้น แม้ในอุปกรณ์ต้นทางหรือปลายทางเจ้าพนักงานอาจพบข้อความที่ถูกบันทึกไว้ก่อนเวลาที่ศาลออกหมายก็ตาม สำหรับการได้มาซึ่งข้อความหรือเนื้อหาของข้อความก่อนที่ศาลจะได้ออกหมายตามมาตรา 100a นี้ จะต้องใช้มาตรการค้นออนไลน์ตามมาตรา 100b

3.2.3 ผู้มีอำนาจอนุมัติให้ใช้มาตรการ

มาตรา 100e วรรคแรก ที่แก้ไขเพิ่มเติมเมื่อเดือนสิงหาคม ค.ศ. 2017 บัญญัติให้อัยการเป็นผู้ร้องขอให้ใช้มาตรการคัดการสื่อสารโทรคมนาคมต่อศาล ในกรณีจำเป็นเร่งด่วน อัยการสามารถอนุญาตให้ใช้มาตรการดังกล่าวได้ แต่หากภายใน 3 วัน ไม่ปรากฏคำอนุมัติจากศาลให้คัดการสื่อสารโทรคมนาคม ให้ถือว่าอนุญาตของอัยการสิ้นสุดลง การอนุมัติให้ใช้มาตรการคัดการสื่อสารโทรคมนาคมสามารถกระทำได้สูงสุดไม่เกิน 3 เดือน โดยไม่ต้องคำนึงว่าโปรแกรมที่ใช้

⁴⁵ BT-Drs. 18/12785 S.51.

ในการดักและบันทึกการสื่อสารได้ถูกติดตั้งเมื่อใด การขอขยายระยะเวลาสามารถกระทำได้ครบเท่าที่เงื่อนไขในการใช้มาตรการยังคงปรากฏอยู่ โดยสามารถขยายได้ครั้งละไม่เกิน 3 เดือน

หมายดักและบันทึกการสื่อสารโทรคมนาคมจะต้องทำเป็นลายลักษณ์อักษร และมีข้อความดังต่อไปนี้ (มาตรา 100e วรรคสาม)

1. ชื่อและที่อยู่ของผู้ที่ได้รับผลกระทบจากการใช้มาตรการ
2. ข้อกล่าวหาที่เป็นฐานของการใช้มาตรการ
3. วิธีการ ขอบเขต ระยะเวลา และเวลาสิ้นสุดของการใช้มาตรการ
4. ประเภทของข้อมูลที่จะได้มาจากการใช้มาตรการและความสำคัญของข้อมูลนั้นต่อการดำเนินคดี
5. เบอร์โทรศัพท์ หรือข้อมูลที่ระบุการเชื่อมต่อที่จะดักและบันทึกการสื่อสาร หรือเครื่องมือหรืออุปกรณ์ปลายทาง

เมื่อศาลอนุมัติแล้ว ผู้ให้บริการการสื่อสารโทรคมนาคมมีหน้าที่ต้องเปิดช่องทางให้หน่วยงานของรัฐสามารถดักและบันทึกการสื่อสารโทรคมนาคมได้ และจะต้องให้ข้อมูลที่เป็นประโยชน์โดยไม่ชักช้า ทั้งนี้ตามมาตรา 100a วรรคสี่ นอกจากนี้ โปรแกรมที่ใช้ในการดักและบันทึกการสื่อสารจะต้องสามารถบันทึกเวลาที่มีการใช้มาตรการ รายละเอียดของข้อมูลที่ระบุถึงระบบเทคโนโลยีสารสนเทศ รายละเอียดที่จะทำให้การดักและบันทึกการสื่อสารเกิดขึ้นได้ และหน่วยงานที่จะเป็นผู้ดำเนินการตามมาตรการ ทั้งนี้ตามมาตรา 100a วรรคหก

ศาลสูงสุดแห่งสหพันธ์เคยวินิจฉัยไว้ว่า แม้ในกรณีที่คุณชนาฝ่ายหนึ่งยินยอมให้มีการดักการสื่อสารโทรคมนาคมได้ ก็ต้องขอ

อนุมัติการดักการสื่อสารโทรคมนาคมจากศาล แต่ในกรณีที่เจ้าหน้าที่ตำรวจแอบฟังอยู่ที่ปลายสายฝั่งหนึ่ง ไม่จำเป็นต้องไปขออนุญาตจากศาลได้⁴⁶

หากเงื่อนไขในการออกหมายไม่ปรากฏอยู่อีกต่อไป มาตรการดักและบันทึกการสื่อสารนั้นจะต้องสิ้นสุดลงโดยมิชักช้า โดยจะต้องแจ้งไปยังศาลผู้ออกหมายด้วย (มาตรา 100e วรคห่า)

เนื่องจากมาตรการดักการสื่อสารโทรคมนาคมจะเกิดขึ้นในทางลับ โดยผู้ที่ได้รับผลกระทบจะไม่สามารถป้องกันหรือขัดขวางมิให้มาตรการนั้นเกิดขึ้นได้ กฎหมายจึงบัญญัติให้ศาลเท่านั้นเป็นผู้ออกหมายอนุมัติให้ใช้มาตรการได้ ซึ่งแสดงให้เห็นถึงการที่กฎหมายพยายามให้องค์กรที่เป็นกลางและอิสระเข้ามาควบคุมว่าองค์กรตำรวจและองค์กรอัยการได้ตรวจสอบการมีอยู่ของเงื่อนไขในการใช้มาตรการหรือไม่

3.2.4 บุคคลผู้ได้รับผลกระทบจากการใช้มาตรการ

ตั้งแต่เมื่อครั้งที่มีการเพิ่มเติมมาตรการดักการสื่อสารโทรคมนาคมลงในประมวลกฎหมายวิธีพิจารณาความอาญาเมื่อปี ค.ศ. 1968 ฝ่ายนิติบัญญัติก็ได้ตระหนักดีอยู่แล้วว่า มาตรการนี้จะไปกระทบต่อสิทธิและเสรีภาพของบุคคลอย่างกว้างขวาง⁴⁷ กล่าวคือ มาตรการนี้ใช้ได้กับทั้งผู้ถูกกล่าวหา ผู้คอยส่งข่าวให้แก่ผู้ถูกกล่าวหา และผู้ที่เป็นเจ้าของระบบการสื่อสารโทรคมนาคมที่ผู้ถูกกล่าวหาใช้ ทั้งนี้ตามมาตรา 100a วรคสามจะเห็นได้ว่า ไม่ว่าจะเป็นบุคคลที่โทรศัพท์หาผู้ถูกกล่าวหาหรือบุคคลที่ผู้ถูกกล่าวหาได้โทรศัพท์หา รัฐก็สามารถดักการสื่อสารโทรคมนาคมของเขาได้ โดยเฉพาะบุคคลประเภทสุดท้ายซึ่งเป็นบุคคลที่ได้รับผลกระทบจากมาตรการดักการสื่อสารโทรคมนาคมนี้อย่างมาก เพราะโดยส่วนใหญ่แล้วเขามักเป็นคนที่ไม่เกี่ยวข้องกับการกระทำความผิดแต่อย่างใด

⁴⁶ BGHSt 39, 335 ff.

⁴⁷ BT-Drs. V/1880.

3.2.5 ข้อมูลที่เกี่ยวข้องกับแกนกลางของการใช้ชีวิตส่วนตัว

มาตรา 100d ประมวลกฎหมายวิธีพิจารณาความอาญา “แกนกลางของการใช้ชีวิตส่วนตัว; สิทธิในการปฏิเสธการเป็นพยาน” ได้บัญญัติวางหลักกฎหมายไว้ในวรรคแรกว่า หากข้อมูลที่จะได้มาจากการดักและบันทึกการสื่อสารโทรคมนาคมเป็นข้อมูลเกี่ยวกับแกนกลางของการใช้ชีวิตส่วนตัว (Kernbereich privater Lebensgestaltung/Core area of private living) การดักและบันทึกการสื่อสารนั้นจะกระทำมิได้ ข้อมูลที่ได้จากการสนทนาระหว่างผู้ที่ถูกกระทบสิทธิกับสมาชิกในครอบครัว ผู้ให้คำปรึกษาทางโทรศัพท์ หน่วยงาน หรือแพทย์ ถือเป็นข้อมูลเกี่ยวกับแกนกลางของการใช้ชีวิตส่วนตัว

ในชั้นของการชั่งน้ำหนักพยานหลักฐาน วรรคสองของมาตรา 100d บัญญัติว่า ข้อเท็จจริงใดๆ ที่เกี่ยวกับแกนกลางของการใช้ชีวิตส่วนตัวที่ได้มาจากการใช้มาตรการดักและบันทึกการสื่อสาร ไม่อาจใช้เป็นพยานหลักฐานในคดีได้และจะต้องถูกลบไปโดยมิชักช้า ข้อเท็จจริงเกี่ยวกับการได้มาและการลบข้อมูลเหล่านั้นจะต้องถูกบันทึกไว้ ทั้งนี้ เพื่อให้ศาลสามารถตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการได้

3.2.6 การตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการ

เพื่อให้เกิดความโปร่งใสและตรวจสอบได้ วรรคสี่แห่งมาตรา 101 จึงบัญญัติให้มีการแจ้งกลับไปยังผู้ที่เข้าร่วมการสื่อสารโทรคมนาคมนั้นว่าได้มีการใช้มาตรการดังกล่าว โดยจะต้องแจ้งสิทธิในการได้รับความคุ้มครองตามกฎหมายตามวรรคเจ็ด และแจ้งระยะเวลาในการใช้สิทธินั้นด้วย คำว่า “ผู้เข้าร่วม” ในการสื่อสารโทรคมนาคมก็หมายถึงผู้ใช้การสื่อสารนั้นนั่นเอง ดังนั้น ในกรณีที่ผู้ถูกกล่าวหาไม่ใช้ผู้ที่ใช้การสื่อสารโทรคมนาคม หรือกรณีที่เจ้าของเบอร์โทรศัพท์มิได้ใช้การสื่อสารนั้นด้วย

ตนเอง เขาทั้งสองก็จะไม่ได้รับการแจ้งตามมาตรา 101 นี้⁴⁸ การแจ้งกลับนี้มีขึ้นเพื่อเป็นหลักประกันแก่หลักฟังความทุกฝ่ายภายหลังจากที่มีการใช้มาตรการแล้ว ทั้งนี้เพื่อเปิดโอกาสให้ผู้ที่ถูกกระทบสิทธิสามารถปกป้องตนเองจากการถูกละเมิดสิทธิได้⁴⁹

อย่างไรก็ตาม การแจ้งกลับอาจจะจับไว้ก่อนได้หากว่าจะเป็นการขัดแย้งกับประโยชน์อื่นตามกฎหมายที่มีคุณค่ามากกว่า อาทิ กรณีที่เป็นการสนทนาระหว่างผู้ส่งข่าวของผู้ถูกกล่าวหากับผู้ที่มีส่วนเกี่ยวข้องกับการทำความผิดด้วย⁵⁰ นอกจากนี้ การแจ้งกลับไปยังผู้เข้าร่วมในการสื่อสารโทรคมนาคมที่การดักการสื่อสารมิได้ทำเพื่อแสวงหาพยานหลักฐานเกี่ยวกับตัวเขา ก็อาจถูกระงับไว้ได้เช่นกันหากว่าสามารถสันนิษฐานได้ว่าบุคคลนั้นไม่ได้สนใจในเรื่องการแจ้งกลับแต่อย่างใด ทั้งนี้เพราะเขาเหล่านั้นเป็นบุคคลผู้ถูกกระทบสิทธิจากการใช้มาตรการน้อยมาก อย่างไรก็ตาม บทบัญญัติวรรคสี่นี้ไม่ใช่บทบังคับศาล แต่เป็นบทบัญญัติที่ให้ศาลใช้ดุลพินิจได้ ดังนั้น แม้บุคคลนั้นจะถูกละเมิดสิทธิเพียงเล็กน้อยและสันนิษฐานได้ว่าเขาไม่ให้ความสนใจที่จะได้รับการแจ้งกลับแต่อย่างใด ศาลก็ยังสามารถสั่งให้มีการแจ้งกลับได้ ในกรณีที่ไม่รู้ตัวผู้เข้าร่วมในการสื่อสารโทรคมนาคม การจะแจ้งกลับจึงกระทำได้ก็ต่อเมื่อต้องมีการสอบสวนหาตัวตนของผู้นั้นให้พบเสียก่อน ศาลรัฐธรรมนูญแห่งสหพันธ์ (Bundesverfassungsgericht - BVerfG) ในคดี BVerfGE 109, 279 ff. จึงได้วางแนวทางไว้และฝ่ายนิติบัญญัติได้นำมาบัญญัติเป็นกฎหมายว่าการสอบสวนเพื่อแสวงหาตัวผู้ที่ใช้การสื่อสารโทรคมนาคมนั้นจะกระทำได้ก็ต่อเมื่อมีความจำเป็นเท่านั้น ทั้งนี้โดยต้องพิจารณาจากความรุนแรงของการละเมิดสิทธิที่เกิดขึ้นกับบุคคลนั้นและภาระที่อาจเกิดขึ้นจากการกระทำเช่นนั้น

⁴⁸ BT-Drs. 16/5846 S.58.

⁴⁹ BGHSt 36, 305, 311.

⁵⁰ BT-Drs. 16/5846 S.59.

การแจ้งกลับต้องกระทำทันทีที่การแจ้งจะไม่ก่อให้เกิดอันตรายต่อเป้าหมายในการการค้นหาคความจริง อันตรายต่อชีวิต ความสมบูรณ์ของร่างกาย เสรีภาพของบุคคลหนึ่งบุคคลใด และทรัพย์สินที่มีความสำคัญ หากมีการเลื่อนการแจ้งกลับเช่นนั้นออกไป ต้องมีการบันทึกการเลื่อนนั้นไว้เป็นลายลักษณ์อักษร (มาตรา 101 วรรคห้า) หากการแจ้งกลับยังคงไม่สามารถกระทำได้ภายใน 12 เดือนหลังจากที่ใช้มาตรการสิ้นสุดลงแล้ว การจะเลื่อนการแจ้งกลับออกไปอีกจะต้องได้รับความเห็นชอบจากศาล และศาลจะเป็นผู้กำหนดระยะเวลาในการเลื่อนการแจ้งกลับนั้น อย่างไรก็ตาม การแจ้งกลับสามารถละทิ้งเสียได้หากเงื่อนไขในการแจ้งจะไม่ปรากฏขึ้นในอนาคตอย่างแน่นอน หากได้มีการใช้มาตรการหลายๆ มาตรการในเวลาใกล้เคียงกัน การนับระยะเวลาแจ้งกลับให้นับตั้งแต่การสิ้นสุดการใช้มาตรการสุดท้าย (มาตรา 101 วรรคหก) ศาลที่มีอำนาจวินิจฉัยตามวรรคหกคือศาลที่มีอำนาจอนุมัติให้ใช้มาตรการผู้เข้าร่วมในการสื่อสารโทรคมนาคมที่ถูกดักฟังสามารถร้องขอให้ศาลตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการ รวมถึงรูปแบบและวิธีการของการใช้มาตรการได้ ในกรณีที่บุคคลตามวรรคสี่ถูกฟ้องเป็นจำเลยต่อศาลแล้ว ให้ศาลที่มีอำนาจพิจารณาคดีอาญาดังกล่าวเป็นผู้พิจารณาคำร้องตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการ (มาตรา 101 วรรคเจ็ด)

3.3 การได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ (Verkehrsdaten)

มาตรา 100g ประมวลกฎหมายวิธีพิจารณาความอาญาให้อำนาจเจ้าพนักงานของรัฐในการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ (Verkehrsdaten/ Call Detail Record) โดยสามารถทำได้ 2 กรณี กรณีแรกตามมาตรา 100g วรรคแรก ซึ่งเป็นการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 96 TKG และกรณีที่สองตามมาตรา 100g วรรคสอง ซึ่งเป็นการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 113b TKG

กรณีแรก การร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 96 TKG ได้แก่ หมายเลขโทรศัพท์ การเชื่อมต่อที่ใช้ หมายเลขลูกค้า สถานที่ตั้งของการเชื่อมต่อสัญญาณโทรศัพท์มือถือ เวลาเริ่มต้นและสิ้นสุดการเชื่อมต่อ หรือปริมาณข้อมูลที่มีการรับส่งกัน เป็นต้น ซึ่งเป็นข้อมูลที่ผู้ให้บริการจะต้องบันทึกไว้เพื่อประกอบกิจการของเขาอยู่แล้ว การร้องขอข้อมูลเหล่านี้จะต้องปรากฏความสงสัยว่าเกิดการกระทำความผิดอาญาตามที่ปรากฏในมาตรา 100a วรรคสอง หรือความผิดอาญาที่อาศัยการสื่อสารโทรคมนาคมในการกระทำความผิด โดยสามารถกระทำได้อีกต่อเมื่อการได้มาด้วยวิธีนี้เป็นกรณีจำเป็นเพื่อให้ได้ข้อเท็จจริงมา และข้อเท็จจริงนั้นมีความสำคัญกับประเด็นของคดีในระดับที่เหมาะสม การร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อโดยอ้างว่ามีความผิดที่อาศัยการสื่อสารโทรคมนาคมในการกระทำความผิดเกิดขึ้น จะต้องปรากฏข้อเท็จจริงด้วยการค้นหาความจริงด้วยวิธีการอื่นไม่อาจเป็นไปได้ ส่วนการร้องขอโดยอ้างว่ามีการกระทำความผิดอาญาตามที่ปรากฏในมาตรา 100a วรรคสองเกิดขึ้น สามารถร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อได้เฉพาะข้อมูลในอนาคตที่กำลังจะเกิดขึ้นหรือข้อมูลที่มีบันทึกอยู่ในขณะที่ร้องขอเท่านั้น และทำได้ก็ต่อเมื่อการค้นหาความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือแทบจะเป็นไปไม่ได้เลย⁵¹

กรณีที่สอง เป็นการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 113b TKG ซึ่งเป็นข้อมูลที่ผู้ให้บริการบันทึกไว้เพราะกฎหมายกำหนดให้กระทำ แต่ในการประกอบกิจการตามปกติแล้ว ไม่ใช่ข้อมูลที่จำเป็นต้องบันทึกไว้แต่อย่างใด การร้องขอข้อมูลประเภทนี้ทำได้ภายใต้เงื่อนไขที่เคร่งครัดกว่าข้อมูลประเภทแรก กล่าวคือ เมื่อมีความสงสัยว่ามีการกระทำความผิดอาญาร้ายแรงตามที่บัญญัติไว้ในวรรคสองของมาตรา 100g นี้เท่านั้น และจะกระทำได้อีกต่อเมื่อการค้นหาความจริงในคดีหรือ

⁵¹ BT-Drs. 18/5088 S.2, 27, 34-35.

การทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือแทบจะเป็นไปไม่ได้เลย และข้อมูลนั้นต้องมีความสำคัญกับประเด็นของคดีในระดับที่เหมาะสม การจัดทำรายงานความเคลื่อนไหว (Bewegungsprofil) ซึ่งต้องอาศัยข้อมูลเกี่ยวกับสถานที่ตั้งของโทรศัพท์มือถือที่ได้มีการบันทึกเอาไว้ ซึ่งเป็นข้อมูลตามมาตรา 113b TKG จึงจะสามารถร้องขอมาได้ก็ต่อเมื่อเข้าเงื่อนไขตามวรรคสองของมาตรา 100g เท่านั้น แตกต่างจากการร้องขอข้อมูลเกี่ยวกับสถานที่ตั้งของโทรศัพท์มือถือซึ่งกำลังจะเกิดขึ้นหรือข้อมูลสถานที่ตั้ง real time ซึ่งเป็นข้อมูลที่ผู้ให้บริการต้องบันทึกไว้อยู่แล้ว จึงสามารถทำได้โดยอาศัยวรรคแรกของมาตรา 100g⁵²

การบัญญัติกฎหมายแยกประเภทของข้อมูลให้ผู้ให้บริการสื่อสารโทรคมนาคมมีหน้าที่จะต้องบันทึกเก็บเอาไว้ออกเป็น 2 ประเภทนี้เป็นผลมาจากคำวินิจฉัยของศาลรัฐธรรมนูญแห่งสหพันธ์ที่ BVerfGE 125, 260 ff. เมื่อปี ค.ศ. 2010 ซึ่งวินิจฉัยว่า บทบัญญัติมาตรา 113a, 113b TKG เดิม ขัดแย้งกับสิทธิในความลับในการสื่อสารทางไกลตามมาตรา 10 วรรคแรก กฎหมายพื้นฐาน ซึ่งคุ้มครองความไว้เนื้อเชื่อใจในการสื่อสารโทรคมนาคมระหว่างบุคคล จึงไม่มีผลบังคับใช้ และนำมาสู่การแก้ไขกฎหมายในปี ค.ศ. 2015 ศาลสูงสุดฯ มองว่า ในการบริหารจัดการการบันทึกข้อมูล จะต้องคำนึงถึงการละเมิดสิทธิขั้นพื้นฐานที่อาจเกิดขึ้นได้เป็นสำคัญ จึงจำเป็นต้องมีบทบัญญัติของกฎหมายที่ชัดเจนเกี่ยวกับการเก็บรักษาข้อมูลให้ปลอดภัย การนำข้อมูลไปใช้ และการตรวจสอบการนำข้อมูลไปใช้ มาตรา 113a และ 113b TKG ที่บัญญัติให้ผู้ให้บริการสื่อสารโทรคมนาคมบันทึกข้อมูลการเชื่อมต่อไว้โดยไม่มีการสร้างความมั่นคงปลอดภัยในการเก็บรักษาข้อมูลและการนำข้อมูลไปใช้ประโยชน์ จึงเป็นบทบัญญัติที่ไม่ชอบด้วยกฎหมายพื้นฐาน

⁵² BT-Drs 18/5088 S.2, 27, 34-35.

เมื่อมีการบัญญัติหน้าที่ในการบริหารจัดการข้อมูลใหม่ตาม มาตรา 113a และ 113b TKG ที่แก้ไขเมื่อปี ค.ศ. 2015 จึงจำเป็นต้องมีการแก้ไขเพิ่มเติมมาตรา 100g ใหม่ด้วย มาตรา 100g ที่ได้แก้ไขใหม่นี้ ช่วยเพิ่มประสิทธิภาพในการดำเนินคดีอาญาด้วย กล่าวคือ มาตรา 100g ก่อนมีการแก้ไขให้อำนาจหน่วยงานของรัฐในการร้องขอข้อมูลการเชื่อมต่อที่ผู้ให้บริการการสื่อสารโทรคมนาคมบันทึกไว้ อย่างไรก็ตาม ผู้ให้บริการการสื่อสารโทรคมนาคมต่างบันทึกข้อมูลเหล่านั้นไว้เป็นระยะเวลาแตกต่างกันตามอำเภอใจของตนเอง เมื่อองค์กรในกระบวนการยุติธรรมร้องขอข้อมูลไป การได้มาซึ่งข้อมูลจึงมีลักษณะขึ้นอยู่กับความบังเอิญว่าในขณะนั้น ผู้ให้บริการโทรคมนาคมมีข้อมูลใดบันทึกเก็บไว้ การแก้ไขกฎหมายในปี ค.ศ. 2015 ที่ได้กำหนดให้เป็นหน้าที่ของผู้ให้บริการการสื่อสารโทรคมนาคมในการบันทึกข้อมูลการเชื่อมต่อเอาไว้ รวมถึงกำหนดระยะเวลาในการบันทึกข้อมูลแต่ละประเภทด้วย ทำให้องค์กรในกระบวนการยุติธรรมสามารถคาดการณ์เพื่อวางแผนการร้องขอข้อมูลได้

ในวรรคสามของมาตรา 100g เป็นบทบัญญัติที่พูดถึงการร้องขอข้อมูลวิเคราะห์จุดรับสัญญาณ (cell site analysis) ซึ่งเป็นการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อที่ปรากฏในจุดรับสัญญาณ ทั้งนี้เพื่อระบุว่าโทรศัพท์มือถือเครื่องใดอยู่ในจุดรับสัญญาณใดในเวลาใดเวลาหนึ่ง ในการร้องขอข้อมูลวิเคราะห์จุดรับสัญญาณนี้ ผู้ร้องขอจะได้ข้อมูลเกี่ยวกับการเชื่อมต่อของบุคคลที่สามที่ใช้โทรศัพท์มือถืออยู่ในขณะนั้นมาด้วย โดยไม่อาจหลีกเลี่ยงได้ การร้องขอข้อมูลวิเคราะห์จุดรับสัญญาณจึงต้องคำนึงถึงหลัก Subsidiarity อย่างเคร่งครัด ภายใต้ข้อจำกัดทางเวลาและสถานที่ที่บัญญัติไว้โดยชัดแจ้งในกฎหมาย ทั้งนี้เพื่อป้องกันมิให้มีการจัดทำรายงานความเคลื่อนไหวของประชาชนผู้บริสุทธิ์

การร้องขอข้อมูลวิเคราะห์จุดรับสัญญาณสามารถทำได้โดยอาศัยเงื่อนไขเดียวกับการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามวรรคแรกของ

มาตรา 100g และทำได้ก็ต่อเมื่อการค้นหาความจริงในคดีหรือการทราบถึงสถานที่ที่ผู้ถูกกล่าวหาพำนักอยู่ทำได้โดยยากลำบากหรือแทบจะเป็นไปไม่ได้เลย โดยจะต้องปรากฏว่าการได้มาซึ่งข้อมูลนั้นมีความสำคัญต่อคดีอย่างมีสัดส่วน

มาตรา 101a บัญญัติให้นำวรรคสามและวรรคสี่ของมาตรา 100a มาใช้กับมาตรการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อด้วย กล่าวคือ การใช้มาตรการนี้สามารถกระทำได้กับผู้ถูกกล่าวหา ผู้คอยส่งข่าวให้แก่ผู้ถูกกล่าวหา และผู้ที่เป็นเจ้าของระบบการสื่อสารโทรคมนาคมที่ผู้ถูกกล่าวหาใช้เท่านั้น (มาตรา 100a วรรคสาม และ 101a วรรคแรก) เมื่อศาลอนุมัติแล้ว ผู้ให้บริการการสื่อสารโทรคมนาคมมีหน้าที่ต้องเปิดช่องทางให้หน่วยงานของรัฐสามารถดักและบันทึกการสื่อสารโทรคมนาคมได้ และจะต้องให้ข้อมูลที่จำเป็นโดยไม่ชักช้า ทั้งนี้ตามมาตรา 100a วรรคสี่ และมาตรา 101a วรรคแรก สำหรับการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 100g วรรคสอง ศาลเท่านั้นที่เป็นผู้ออกหมายอนุมัติให้กระทำได้ อัยการไม่อาจออกหมายอนุมัติให้ร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 100g วรรคสอง โดยอาศัยเหตุจำเป็นเร่งด่วนได้

ศาลจะอนุมัติให้มีการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อหรือ ยึดระยะเวลาการร้องขอได้ก็ต่อเจ้าหน้าที่แสดงเหตุผลมาเป็นกรณีพิเศษถึงความจำเป็นและความเหมาะสมของการใช้มาตรการของคดีนั้นๆ รวมถึงต้องให้เหตุผลพิเศษเกี่ยวกับขอบเขตของข้อมูลที่จะได้มาและระยะเวลาที่จะร้องขอด้วย (วรรคสอง แห่งมาตรา 101a) การที่กฎหมายบัญญัติให้มีการให้เหตุผลพิเศษนี้แสดงให้เห็นถึงการที่กฎหมายพยายามเพิ่มการตรวจสอบการใช้มาตรการโดยศาล และเพิ่มความคุ้มครองตามกฎหมายให้แก่ผู้ถูกระทบสิทธิตนเอง



4. การใช้และการเก็บรักษาข้อมูลที่ได้จากการใช้มาตรการ

ประมวลกฎหมายวิธีพิจารณาความอาญาเยอรมันได้บัญญัติถึงการใช้และเก็บรักษาข้อมูลที่ได้จากการดักการสื่อสารโทรคมนาคมและจากการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อเอาไว้ในมาตรา 101 และ 101a

4.1 กรณีการดักและบันทึกการสื่อสารโทรคมนาคม

มาตรา 101 “กฎเกณฑ์ในการดำเนินการตามมาตรการที่กระทำโดยลับ” ถูกแก้ไขครั้งสำคัญเมื่อปี ค.ศ. 2008 ด้วยกฎหมายว่าด้วยกฎเกณฑ์ใหม่ในการดักการสื่อสารโทรคมนาคมและมาตรการในการสอบสวนที่กระทำโดยลับและเพื่อการปรับใช้คำสั่งของสหภาพยุโรป 2006/24/EG (Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahme sowie zur Umsetzung der Richtlinie 2006/24/EG) ทั้งนี้เพื่อให้บทบัญญัติเกี่ยวกับมาตรการทางอาญาต่างๆ สอดคล้องกันและเพื่อบริหารจัดการให้เป็นไปตามแนวทางที่ศาลรัฐธรรมนูญแห่งสหพันธ์ (BVerfG) ได้เคยวินิจฉัยเอาไว้ กล่าวคือเพิ่มความคุ้มครองตามกฎหมายให้แก่ผู้ที่ถูกละเมิดสิทธิจากการใช้มาตรการ กำจัดความไม่ชัดเจนและช่องว่างทางกฎหมาย รวมถึงแก้ไขให้กฎหมายโปร่งใสและปฏิบัติได้จริงมากขึ้น⁵³ โดยมาตรา 101 เป็นบทบัญญัติกลางสำหรับการใช้มาตรการทางอาญาที่กระทำโดยลับหลายๆ มาตรการ เช่น การค้นออนไลน์ (มาตรา 100b) การแอบฟังในโทรศัพท์ (มาตรา 100c) หรือการแฝงตัว (มาตรา 110a) และรวมถึงมาตรการดักฟังการสื่อสารโทรคมนาคมตามมาตรา 100a ด้วย

วรรคสามแห่งมาตรา 101 StPO ซึ่งแก้ไขตามคำวินิจฉัยของศาลรัฐธรรมนูญแห่งสหพันธ์ที่ BVerfGE 100, 313 ff. และ BVerfGE 109, 279 ff. บัญญัติถึงหน้าที่ในการทำเครื่องหมายแสดงให้เห็นว่าข้อมูล

⁵³ BT-Drs. 16/5846 S.22.

ใดเป็นข้อมูลที่ได้มาจากการดักฟังการสื่อสารโทรคมนาคมตาม และแม้จะได้มีการส่งต่อข้อมูลเช่นว่านั้นไปยังหน่วยงานอื่น การทำเครื่องหมายแสดงข้อมูลก็ให้คงไว้เช่นเดิมต่อไป

มาตรา 101 วรรคแปด บัญญัติว่า ข้อมูลส่วนบุคคลที่ได้มาจากการใช้มาตรการดักการสื่อสารโทรคมนาคมที่ไม่จำเป็นสำหรับการดำเนินคดีอาญาและการตรวจสอบการใช้มาตรการโดยศาลแล้วอีกต่อไปนั้น ให้ลบเสียโดยมิชักช้า การลบข้อมูลเหล่านั้นจะต้องถูกบันทึกไว้เป็นลายลักษณ์อักษรทราบได้ก็ตามที่การลบข้อมูลส่วนบุคคลนั้นถูกเลื่อนออกไปเพราะรอการตรวจสอบความชอบด้วยกฎหมายของการใช้มาตรการโดยศาล ข้อมูลเหล่านั้นอาจจะถูกนำมาใช้ได้โดยไม่ต้องขอความยินยอมจากเจ้าของข้อมูลเพียงเพื่อการนั้นเท่านั้น

4.2 กรณีการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อ

สำหรับมาตรการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อนั้น ไม่สามารถใช้บทบัญญัติกลางมาตรา 101 ประมวลกฎหมายวิธีพิจารณาความอาญาได้ ทั้งนี้เพราะศาลรัฐธรรมนูญแห่งสหพันธ์ได้เคยวินิจฉัยวางหลักกฎหมายไว้ในคดี BVerfGE 125, 260 ff. ว่า การดำเนินการตามมาตรการได้มาซึ่งข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 101a นั้น โดยหลักจะต้องทำโดยเปิดเผย ทั้งนี้ตามหลักการตรงไปตรงมาในการได้มา และใช้ข้อมูลส่วนบุคคล (Grundsatz der Offenheit der Erhebung und Nutzung von personenbezogenen Daten) ข้อมูลส่วนบุคคลที่ได้มาจากการใช้มาตรการตามมาตรา 100g นี้จะต้องถูกทำเครื่องหมายระบุไว้ให้ชัดเจน และจะต้องถูกนำไปใช้โดยมิชักช้า ทั้งนี้เพื่อเป็นหลักประกันว่าการละเมิดสิทธิส่วนบุคคลที่อาจเกิดจากการใช้ข้อมูลนั้นจะไม่คงอยู่ถาวร และจะไม่มี ความเข้มข้นมากขึ้น⁵⁴ และหากเป็นข้อมูลส่วนบุคคลตามมาตรา 113b TKG จะต้องมีการระบุไว้เป็นพิเศษเพิ่มเติมขึ้นอีกด้วย

⁵⁴ BT-Drs. 18/5088 S.35.

การลบข้อมูลส่วนบุคคลเหล่านั้นมาตรา 101a บัญญัติให้นำมาตรา 101 วรรคแปดมาใช้ ซึ่งหมายความว่า ข้อมูลเกี่ยวกับการเชื่อมต่อที่แม่ไม่ได้บันทึกไว้ตามมาตรา 113b TKG ก็จะต้องปฏิบัติตามวรรคแปดของมาตรา 101 ด้วย ทั้งนี้เพราะไม่ว่าจะเป็นข้อมูลประเภทใด การบันทึกข้อมูลไว้ถาวรย่อมเป็นการละเมิดสิทธิของเจ้าของข้อมูลนั้น ทั้งการบัญญัติกฎหมายให้ลบข้อมูลทุกประเภทนี้ยังง่ายต่อการปฏิบัติด้วย⁵⁵

ในวรรคสี่แห่งมาตรา 101a บัญญัติว่า ข้อมูลส่วนบุคคลที่ได้มาตามมาตรา 100g วรรคสองและวรรคสาม สามารถนำไปใช้ในการพิจารณาพิพากษาคดีได้โดยปราศจากความยินยอมของผู้เข้าร่วมการสื่อสารโทรคมนาคมได้ตามเพียงวัตถุประสงค์ที่ระบุไว้ในวรรคสี่ของมาตรา 101a เท่านั้น กล่าวคือ 1) ใช้ในการค้นหาความจริงในคดีอาญาอื่นที่สามารถใช้มาตรการตามมาตรา 100g วรรคสองในการค้นหาความจริงได้เช่นกัน หรือเพื่อทราบสถานที่อยู่ของผู้ถูกกล่าวหาในคดีนั้น หรือ 2) ใช้เพื่อป้องกันอันตรายต่อชีวิต ร่างกาย และเสรีภาพของบุคคลคนหนึ่งหรือเพื่อความคงอยู่ของสหพันธ์หรือมลรัฐหนึ่งมลรัฐใด

วรรคห้าแห่งมาตรา 101a บัญญัติถึงกรณีการนำข้อมูลเกี่ยวกับการเชื่อมต่อตามมาตรา 113b TKG ที่บันทึกไว้เพื่อป้องกันการกระทำความผิดอาญามาใช้ในการดำเนินคดีอาญา ซึ่งจะสามารถทำได้ก็ต่อเมื่อมาตรการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อนี้สามารถทำได้ในคดีนั้นเช่นกัน

ตามหลักฟังความทุกฝ่าย ผู้ที่ถูกกระทบสิทธิจะต้องสามารถยกข้ออ้างและข้อเถียงของตนขึ้นคัดค้านการออกหมายตามมาตรา 100g ได้ วรรคหกแห่งมาตรา 101a จึงบัญญัติว่า ผู้ที่เข้าร่วมในการสื่อสารโทรคมนาคมจะต้องได้รับการแจ้งว่ามีการร้องขอข้อมูลเกี่ยวกับการเชื่อมต่อ โดยให้นำเอามาตรา 101 วรรคสี่ถึงวรรคเจ็ดมาใช้ เมื่อศาลได้ออกหมายแล้ว ศาลจะส่งหมายให้อัยการและอัยการมีหน้าที่ดำเนินการให้เป็นไปตามหมายนั้น

⁵⁵ BT-Drs. 18/5088 S.35.



5. ความรับผิดทางอาญาเกี่ยวกับการได้มาโดยไม่ชอบซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกัน

ความรับผิดทางอาญาที่เกี่ยวกับการได้มาโดยไม่ชอบซึ่งข้อมูลส่วนบุคคลสื่อสารถึงกัน ปรากฏอยู่ในประมวลกฎหมายอาญาเยอรมัน (Strafgesetzbuch - StGB) ลักษณะที่ 15 การล่วงละเมิดพื้นที่ในการใช้ชีวิตส่วนตัวและในความลับมาตรา 201 ถึง 210 โดยมีฐานความผิดที่เกี่ยวข้องดังต่อไปนี้

5.1 ความผิดฐานล่วงล้ำความเป็นส่วนตัวของคำพูด

ความผิดฐานล่วงล้ำความเป็นส่วนตัวของคำพูด ตามมาตรา 201 ประมวลกฎหมายอาญา (Strafgesetzbuch - StGB) คื้มครองความเป็นส่วนตัวของคำพูดในแง่ที่เป็นสิ่งที่ลอยหายไปโดยรวดเร็ว พ้นจากความเป็นไปได้ในการยึดถือและรักษาไว้ด้วยวิธีการทางเทคนิคใดๆ จึงเป็นความผิดที่คุ้มครองความเป็นส่วนตัวของบุคคลจากการถูกล่วงละเมิดในการดำรงชีวิตในสังคมและการติดต่อสื่อสารกันระหว่างคนในสังคม ไม่ควรมีผู้ใดต้องคอยระวังว่าคำพูดของตนจะถูกเปิดเผยออกไปและจะถูกแปลงให้อยู่ในรูปของเทปบันทึกเสียงที่สามารถเล่นซ้ำเมื่อใดก็ได้⁵⁶ ในการสนทนาโดยปกติ บุคลิกลักษณะของผู้พูดจะถูกถ่ายทอดออกไปด้วย ดังนั้นผู้พูดเท่านั้นที่จะมีสิทธิกำหนดขอบเขตของคำพูดของเขา ขอบเขตของผู้สนทนา และรวมถึงกำหนดด้วยว่าคำพูดของเขาควรถูกบันทึกลงในแถบบันทึกเสียงหรือไม่⁵⁷

วัตถุประสงค์ของการกระทำตามมาตรา 201 นี้คือ ถ้อยคำที่ได้พูดออกไปในลักษณะส่วนตัว ทั้งนี้โดยกฎหมายไม่สนใจว่าถ้อยคำที่พูดออกไปนั้นจะเป็นความจริงหรือไม่⁵⁸ “ถ้อยคำที่พูดออกไป” หมายความว่าถึง

⁵⁶ Gallas, ZStW 1963, 16 ff.; Wessels/Hettinger, § 12, Rn.525.

⁵⁷ BVerfGE 34, 238; BVerfG NJW 92, 815; BGHSt 14, 358.

⁵⁸ Wessels/Hettinger, § 12, Rn.525.

การแสดงออกทางความคิดโดยใช้คำพูด ดังนั้น การแสดงออกที่ไม่ใช้คำพูด เช่น ด้วยท่าทาง หรือการปล่อยเสียงออก เช่น ถอนหายใจ ตะโกน หรือ หาว จึงไม่ใช่วัตถุของการกระทำตามมาตรานี้ เช่นเดียวกับการถ่ายภาพ หรือถ่ายวิดีโอ และรวมถึงเสียงของเครื่องดนตรีด้วย⁵⁹

ถ้อยคำได้ถูกพูดออกไปในลักษณะ “ส่วนตัว” เมื่อผู้พูดยังสามารถควบคุมขอบเขตของการพูดได้ ดังนั้น การพูดจึงยังคงมีลักษณะส่วนตัวอยู่แม้ว่าจะได้พูดต่อหน้ากลุ่มผู้ฟังจำนวนมาก แต่ผู้พูดยังคงควบคุมอาณาเขตของการสื่อสารได้อยู่ การพูดที่เป็นสาธารณะคือการพูดในโอกาสที่ใครก็ตามสามารถเข้าร่วมฟังได้ การพูดในการพิจารณาคดีที่กระทำโดยเปิดเผยจึงไม่อาจเป็นวัตถุของการกระทำตามมาตรานี้ได้⁶⁰ การพูดจะไม่กลายเป็นสาธารณะเพียงเพราะการพูดนั้นสามารถถูกแอบฟังได้โดยง่าย และไม่มีผู้ใดสังเกต อย่างไรก็ตาม การพูดจะไม่มีลักษณะส่วนตัวอีกต่อไป หากว่าคนจำนวนหนึ่งที่สามารถได้ยินคำพูดนั้นได้โดยไม่ต้องใช้ความพยายามใดๆ เป็นพิเศษ เช่น กรณีทนายความพูดเกี่ยวกับลูกความ เสียงดังหน้าห้องพิจารณา การพูดคุยผ่านคลื่นวิทยุสื่อสารไม่ถือเป็นการพูดที่มีลักษณะส่วนตัวเพราะใครๆ ก็สามารถฟังได้โดยใช้เครื่องมือหรืออุปกรณ์ที่จำเป็น

การกระทำที่เป็นความผิดฐานนี้มี 4 ประการ ได้แก่

1. การบันทึกเสียงลงบนเทปบันทึกเสียงโดยไม่ได้รับอนุญาต (วรรคแรก ข้อ 1.)
2. การใช้เทปบันทึกเสียงหรือการทำให้บุคคลที่สามเข้าถึงเทปบันทึกเสียงนั้นโดยไม่ได้รับอนุญาต (วรรคแรก ข้อ 2.) การ “ใช้” เทปบันทึกเสียงโดยไม่ได้รับอนุญาต หมายถึง การรับรู้เนื้อหาของ

⁵⁹ Kindhäuser, BT I, § 28, Rn.3.

⁶⁰ Kindhäuser, BT I, § 28, Rn.4.

เทปบันทึกเสียงด้วยการเล่นเทปนั้น ดังนั้น การถอดเทปที่ถูกบันทึกไว้โดยไม่ได้รับอนุญาตออกมาอยู่ในรูปเอกสารและเผยแพร่เอกสารนั้น จึงไม่มีความผิดตามมาตรา 201 นี้ การทำให้บุคคลที่สาม “เข้าถึง” เทปบันทึกเสียงโดยไม่ได้รับอนุญาต หมายถึง บุคคลที่สามรู้เนื้อหาในเทปบันทึกเสียงนั้นผ่านการเล่นเทป หรือผู้กระทำความผิดมอบเทปบันทึกเสียงให้บุคคลที่สามนำเอาไปใช้ได้⁶¹

3. การแอบฟังคำพูดที่เป็นส่วนตัวที่ไม่ต้องการให้ผู้กระทำความผิดล่วงรู้โดยอาศัยอุปกรณ์ในการแอบฟัง (วรรคสอง ข้อ 1.) คำพูดที่ผู้พูด “ไม่ต้องการให้ผู้กระทำความผิดล่วงรู้” หมายถึงกรณีที่ผู้กระทำความผิดไม่ได้อยู่ในขอบเขตของผู้ฟังที่ผู้พูดได้กำหนดไว้ อุปกรณ์ในการแอบฟังหมายถึง เครื่องมือที่ทำให้สามารถรับฟังการพูดได้โดยการเพิ่มเสียง เช่น ไมโครโฟน หรือ FM transmitter เป็นต้น ดังนั้น ผู้ที่เพียงเอาหูแนบกับผนังเพื่อแอบฟังจึงไม่มีความผิดตามมาตรา 201 นี้ แต่หากว่ามีการนำเอา ear trumpet มาใช้ ก็ถือว่ามีความผิดตามมาตรา 201 นี้ การ “แอบฟัง” หมายถึง การรับรู้การพูดนั้นโดยตรง และรวมถึงการบันทึกเสียงผ่านอุปกรณ์แอบฟังด้วย⁶²

4. การบอกคำพูดที่เป็นส่วนตัวที่ถูกบันทึกไว้ตามวรรคแรก ข้อ 1. และถูกแอบฟังตามวรรคสอง ข้อ 1. แก่บุคคลที่สาม โดยเป็นการบอกอย่างเปิดเผย ซึ่งหมายความว่า เป็นการบอกแก่กลุ่มผู้ฟังจำนวนมาก แต่ไม่รู้จำนวนที่แน่นอน และไม่ได้มีความเกี่ยวพันกันอย่างใกล้ชิด⁶³

ผู้กระทำความผิดตามมาตรา 201 จะต้องกระทำโดยไม่ได้รับอนุญาต ประเด็นนี้เป็นประเด็นปัญหาที่ถกเถียงกันในหมู่นักกฎหมาย

⁶¹ Kindhäuser, BT I, § 28, Rn.8-10.

⁶² Kindhäuser, BT I, § 28, Rn.11-15.

⁶³ Kindhäuser, BT I, § 28, Rn.16-17.

ชาวเยอรมันว่า ความยินยอมของผู้ที่ถูกกระทำความผิดตามมาตรานี้ทำให้การกระทำขาดองค์ประกอบความผิด หรือทำให้ผู้กระทำความผิดมีอำนาจกระทำได้อันทำให้การกระทำไม่เป็นความผิด นักกฎหมายฝ่ายข้างมาก⁶⁴ เห็นว่าถ้อยคำว่า “โดยไม่ได้รับอนุญาต” ในความผิดตามมาตรา 201 นี้ ไม่ใช่องค์ประกอบความผิด เป็นแต่เพียงถ้อยคำที่ฝ่ายนิติบัญญัติชี้ให้เห็นถึงความผิดกฎหมาย (Wrongdoing/ Unrecht) ของการกระทำความผิดตามโครงสร้างความรับผิดชอบทางอาญาข้อที่ 2 เท่านั้น ดังนั้น ในกรณีที่ผู้กระทำความผิดตามกฎหมาย อาทิ กฎหมายวิธีพิจารณาความอาญาที่ให้อำนาจเจ้าพนักงานตักการสื่อสารโทรคมนาคมได้ การกระทำจึงไม่เป็นความผิด

5.2 ความผิดฐานล่วงรู้ความลับในจดหมาย

ความผิดฐานล่วงรู้ความลับในจดหมาย ตามมาตรา 202 ประมวลกฎหมายอาญา เป็นบทบัญญัติที่คุ้มครองความลับในจดหมายในฐานะที่เป็นส่วนหนึ่งของสิทธิในพื้นที่ส่วนตัว ข้อมูลที่ปรากฏในจดหมายจะต้องได้รับความคุ้มครองมิให้ผู้ที่ไม่ได้รับอนุญาตล่วงรู้ได้⁶⁵ ความผิดฐานนี้เป็นความผิดที่ต้องมีคำร้องทุกข์ เจ้าพนักงานจึงจะสามารถดำเนินคดีได้ (มาตรา 205)

การกระทำที่เป็นความผิดฐานนี้มี 3 ประการ ได้แก่

1. การเปิดจดหมายหรือเอกสารอื่นที่ปิดผนึกไว้เพื่อป้องกันมิให้ผู้กระทำความผิดล่วงรู้ (วรรคแรก ข้อ 1.) จดหมายหรือเอกสารอื่นจะเป็นเอกสาร “ปิดผนึก” ก็ต่อเมื่อมีการใช้วิธีการป้องกันอย่างหนึ่งอย่างใดที่เป็นการขัดขวางมิให้ผู้อื่นล่วงรู้ถึงเนื้อหาในเอกสารนั้น จดหมายหรือเอกสารอื่นจะเป็นเอกสารที่ “มิได้มุ่งหมายให้ผู้กระทำความผิดล่วงรู้” ก็ต่อเมื่อผู้มีสิทธิมิได้ต้องการให้เนื้อหาของเอกสารนั้นล่วงรู้ถึงผู้กระทำความผิด

⁶⁴ BGHSt 31, 304, 306; LK-Schünemann, § 201, Rn.9, 27; ความเห็นข้างน้อยโปรดดู Wessels/Hettinger, § 12, Rn.534.

⁶⁵ Kindhäuser, BT I. § 29, Rn.1; Wessels/Hettinger, § 12, Rn.547.

ผู้มีสิทธิก็คือผู้ส่งในกรณีที่เอกสารยังไม่ไปถึงผู้รับ และคือผู้รับในกรณีที่เอกสารไปถึงผู้รับแล้ว การ “เปิด” หมายถึง การกระทำใดๆ ที่ทำให้เกิดความเป็นไปได้ในการรู้ข้อความในจดหมายหรือเอกสาร แต่ผู้กระทำไม่จำเป็นต้องรู้ข้อความนั้นก็ได้⁶⁶

2. การล่วงรู้เนื้อหาในจดหมายหรือเอกสารโดยการใช้วิธีทางเทคนิคโดยไม่จำเป็นต้องเปิดผนึกจดหมายหรือเอกสารนั้น (วรรคแรกข้อ 2.) การรับรู้เพียงด้วยการเห็นเอกสารทั้งหมดหรือบางส่วนก็ถือเป็น การรู้ตามความหมายนี้แล้ว ผู้กระทำไม่จำเป็นต้องเข้าใจเนื้อหาของเอกสารนั้น ดังนั้น เมื่อผู้กระทำเปิดจดหมายที่ปิดผนึกออกแล้ว ก็ถือว่าผู้กระทำได้ล่วงรู้ข้อความในเอกสารนั้นแล้วแม้ว่าเอกสารจะเป็นภาษาต่างประเทศที่อ่านไม่เข้าใจก็ตาม การล่วงรู้เนื้อหาในเอกสารโดยการใช้ “วิธีการทางเทคนิค” หมายความว่า การใช้วัสดุหรือเครื่องมือพิเศษเพื่อเห็นข้อความในเอกสารนั้น อาทิ ใช้สารเคมีหรือใช้รังสีส่องลงบนเอกสาร แต่การที่ผู้กระทำเพียงใช้แสงจากคอมไฟส่องลงบนเอกสารเพื่ออ่านข้อความในเอกสารนั้น ยังไม่ถือว่าเป็นการใช้วิธีการทางเทคนิคแต่อย่างใด⁶⁷

3. การล่วงรู้เนื้อหาในเอกสารที่คุ้มครองไว้เป็นพิเศษด้วยการใส่ภาษาที่ลึกลับเพื่อป้องกันมิให้ผู้อื่นเห็นเนื้อหาของเอกสารนั้น หลังจากที่ผู้กระทำได้เปิดภาษานั้นแล้ว ภาษาที่ลึกลับ หมายความว่า สิ่งของที่มีลักษณะ 3 มิติที่มีไว้เพื่อป้องกันการล่วงล้ำของมนุษย์และเพื่อเก็บรักษาสิ่งของ เช่น ลิ้นชัก ตู้ ตู้นิรภัย แต่ไม่รวมถึงห้องที่ลึกลับ ภาษาที่มีหน้าที่ในการ “คุ้มครองเป็นพิเศษ” เมื่อภาษานั้นถูกปิดเอาไว้เพื่อป้องกันการล่วงรู้เอกสารที่ถูกเก็บรักษาไว้ข้างใน⁶⁸

⁶⁶ Kindhäuser, § 29, Rn.4-7.

⁶⁷ Kindhäuser, § 29, Rn.12.

⁶⁸ Kindhäuser, § 29, Rn.13-16.



6. หลักเกณฑ์การรับฟังข้อมูลต่อบุคคลสื่อสารถึงกัน เป็นพยานหลักฐาน

ประมวลกฎหมายวิธีพิจารณาความอาญามิได้บัญญัติว่า ข้อมูลที่ได้มาจากการใช้มาตรการดักการสื่อสารโทรคมนาคมนี้จะถูกนำเสนอเข้าไปในคดีอย่างไร แต่ศาลสูงสุดแห่งสหพันธ์เคยวางหลักไว้ว่า อัยการสามารถนำเสนอข้อมูลที่ได้จากการดักการสื่อสารโทรคมนาคมได้ในฐานะเป็นพยานวัตถุด้วยการเปิดเทปบันทึกเสียงในห้องพิจารณา หรือในฐานะเป็นพยานเอกสารด้วยการถอดเทปออกมาเป็นเอกสารก็ได้⁶⁹

ส่วนประเด็นข้อห้ามการชักนำพยานหลักฐาน⁷⁰ ที่เกิดจากการได้มาซึ่งพยานหลักฐานโดยมิชอบนั้น เป็นประเด็นที่มีข้อถกเถียงกันมายาวนาน นักกฎหมายในเยอรมนีพยายามนำเสนอทฤษฎีต่างๆ ไว้มากมายหลายทฤษฎี โดยมีทฤษฎีสำคัญๆ ที่ควรกล่าวถึงอยู่ด้วยกัน 3 ทฤษฎี

1) ทฤษฎีขอบเขตแห่งสิทธิตามกฎหมาย (Rechtskristheorie)

ทฤษฎีนี้จะพิจารณาว่าการฝ่าฝืนกฎเกณฑ์การนำสืบพยานหลักฐานก่อให้เกิดความเสียหายต่อสิทธิของผู้ถูกกล่าวหาหรือไม่ เฉพาะการฝ่าฝืนกฎเกณฑ์การนำสืบพยานหลักฐานที่สร้างความเสียหายแก่สิทธิของผู้ถูกกล่าวหาเท่านั้น จึงจะนำไปสู่การห้ามมิให้ศาลใช้ผลลัพธ์ในการนำสืบพยานหลักฐานนั้น⁷¹ ยกตัวอย่างเช่น ในกรณีที่ศาลไม่เตือนพยานถึงคำถามที่อาจ

⁶⁹ BGHSt 27, 135; BGH NStZ 08, 230; 09, 280.

⁷⁰ ในประเทศเยอรมนี มีการพูดถึงข้อห้ามการรับฟังพยานหลักฐาน (Beweisaufnahme/Admissibility of Evidence) ค่อนข้างน้อย แต่ไปเน้นพูดถึงข้อห้ามการชักนำพยานหลักฐาน (Beweisverwertung/ Evaluation of Evidence) มากกว่า

⁷¹ BGHSt (GrS) 11, 213, 215; 38, 214, 220; Bauer, NJW 1994, 2530 f.

ทำให้เขาถูกฟ้องคดีอาญา เช่นนี้ ผู้ที่ได้รับความเสียหายไม่ใช่ผู้ถูกกล่าวหา แต่เป็นพยาน ศาลจึงสามารถนำถ้อยคำของพยานบุคคลนั้นไปใช้ได้ หากพิจารณาตามทฤษฎีนี้

ทฤษฎีนี้มักถูกโต้แย้งว่า ผู้ถูกกล่าวหาไม่ได้มีเพียงสิทธิที่จะเรียกร้องให้กระบวนการยุติธรรมปฏิบัติตามบทบัญญัติของกฎหมายที่คุ้มครองสิทธิของเขาเท่านั้น แต่เขายังมีสิทธิที่จะเรียกร้องให้การดำเนินคดีอาญาเป็นไปอย่างถูกต้องตามบทบัญญัติของกฎหมายด้วยแม้ว่ากฎหมายนั้นจะมีได้คุ้มครองสิทธิของเขาก็ตาม⁷²

คำวินิจฉัยของศาลสูงสุดแห่งสหพันธ์ตั้งแต่ปี ค.ศ. 1971 เป็นต้นมา ไม่เคยวินิจฉัยเรื่องข้อห้ามการขังน้ำหนักพยานหลักฐานโดยใช้ทฤษฎีนี้อีกเลย นักกฎหมายเยอรมันบางคนถึงกับกล่าวว่า “ทฤษฎีนี้ได้ตายจากโลกนี้ไปแล้ว” เสียด้วยซ้ำ⁷³

2) ทฤษฎีเป้าหมายที่คุ้มครอง (Schutzzwecktheorie)

ทฤษฎีเป้าหมายที่คุ้มครองนี้กำหนดข้อห้ามการขังน้ำหนักพยานหลักฐานจากเป้าหมายที่กฎเกณฑ์การนำสืบพยานหลักฐานประสงค์จะคุ้มครอง หากกฎเกณฑ์การนำสืบพยานหลักฐานมีขึ้นเพราะไม่ต้องการให้ศาลใช้พยานหลักฐานเหล่านั้นในการพิจารณาพิพากษาคดี การฝ่าฝืนกฎเกณฑ์การนำสืบพยานหลักฐานนั้นก็จะมีผลห้ามมิให้ศาลใช้พยานหลักฐานนั้นในการพิจารณาพิพากษาคดี⁷⁴ ยกตัวอย่างเช่น กรณีเอกสารโต้ตอบระหว่างผู้ต้องหาหรือจำเลยกับทนายความตามมาตรา 97 I StPO กฎหมาย

⁷² Eisenberg, Rn.365; Fezer, JuS 1978, 104, 127; Geppert, Jura 1988, 305, 313; Roxin/Schünemann, § 24, Rn. 24; Eb. Schmidt, JZ 1958, 596.

⁷³ Rogall, ZStW 1979, 1, 26.

⁷⁴ Amelung, NJW 1991, 2533 ff.; Beulke, § 23, Rn.458; Grünwald, S.143 ff.; Jäger, S.131 ff.; KMR-Paulus, § 244, Rn.516 ff.; Roxin/Schünemann, § 24, Rn.24.

มีการให้เอกสารเหล่านั้นตกมาอยู่ในมือของกระบวนการยุติธรรมและถูกนำไปใช้ในการพิจารณาพิพากษาความผิดของจำเลย ข้อห้ามมิให้ค้นและยึดเอกสารเหล่านี้จึงควรจะขัดขวางมิให้เอกสารดังกล่าวถูกนำมาใช้ในการพิจารณาพิพากษาคดี ทำนองเดียวกันกับมาตรา 105 วรรคท้าย ป.วิ.อ.

ทฤษฎีเป้าหมายที่คุ้มครองนี้ถูกวิพากษ์วิจารณ์ว่ามีปัญหาในบังคับใช้ กล่าวคือ ในหลายกรณี เราไม่อาจทราบได้ว่ากฎเกณฑ์การนำสืบพยานมีเป้าหมายในการคุ้มครองสิ่งใด⁷⁵ อีกทั้ง ข้อห้ามการขังน้ำหนักรพยานหลักฐานก็มิได้เกิดจากเป้าหมายเพียงประการใดประการหนึ่ง ยังมีหลักเกณฑ์อื่นๆ อีกที่เป็นเกณฑ์กำหนดข้อห้ามการขังน้ำหนักรพยานหลักฐาน เช่น กรณีมีการฝ่าฝืนบทบัญญัติแห่งกฎหมายวิธีพิจารณาความอาญาอันส่งผลให้ความชอบธรรมของการดำเนินคดีอาญาสิ้นคลอน

3) ทฤษฎีการขังน้ำหนัก (Abwägungstheorie)

ความเห็นฝ่ายข้างมากในประเทศเยอรมนี⁷⁶ เสนอให้มีการขังน้ำหนักคุณค่าที่กฎหมายวิธีพิจารณาความอาญาคู่ครองอย่างละเอียดถี่ถ้วน แล้วเปรียบเทียบข้อดีข้อเสียกัน คุณค่าด้านหนึ่งคือ ประโยชน์ส่วนบุคคลของผู้ถูกกล่าวหา ซึ่งอาจพิจารณาจากความรุนแรงของการฝ่าฝืนกฎเกณฑ์การนำสืบพยานหลักฐาน ส่วนคุณค่าอีกด้านหนึ่งคือ ประโยชน์ที่จะได้จากการดำเนินคดีอาญาที่มีประสิทธิภาพ ซึ่งอาจพิจารณาจากความร้ายแรงของการกระทำความผิด โดยให้พิจารณาจากความร้ายแรงของการกระทำความผิดนั้นๆ ที่เกิดขึ้นจริง มิใช่ความร้ายแรงของการกระทำความผิดในลักษณะนามธรรม⁷⁷ ในกรณีคดีอาญาร้ายแรง ศาลจึงมักจะไม่ปฏิเสธ ที่จะใช้พยานหลักฐานที่น่าสืบมาโดยฝ่าฝืนกฎเกณฑ์การนำสืบพยานหลักฐาน

⁷⁵ Eisenberg, Rn.366; Volk/Engländer, § 28, Rn.10.

⁷⁶ BGHSt 42, 372, 377; 47; 172, 179; LR-Gössel, Einleitung, Abschnitt L, Rn.155; Rogall, NStZ 1988, 385, 392.

⁷⁷ BVerfGE 34, 250; BGHSt 19, 322 ff.

ทฤษฎีการชั่งน้ำหนักนี้ถูกวิพากษ์วิจารณ์ว่าขาดความชัดเจนแน่นอนในการปรับใช้และไม่สามารถคาดการณ์ผลของการชั่งน้ำหนักไว้ล่วงหน้าได้เลย⁷⁸ นักกฎหมายบางท่านโต้แย้งต่อไปอีกว่า การชั่งน้ำหนักคุณค่าที่วุ่นนี้ได้เกิดขึ้นแล้วโดยบทบัญญัติห้ามการนำสืบพยานหลักฐานนั่นเอง⁷⁹

กล่าวโดยสรุปได้ว่า ฝ่ายตำรากียังไม่อาจพัฒนาหลักกฎหมายที่สามารถใช้เป็นหลักเกณฑ์ในการวินิจฉัยที่สามารถนำไปปฏิบัติได้จริง⁸⁰ ส่วนฝ่ายศาลก็ใช้วิธีชั่งน้ำหนักระหว่างประโยชน์ส่วนรวมกับประโยชน์ส่วนตัวเป็นกรณีๆ ไป

⁷⁸ Eisenberg, Rn.367.

⁷⁹ Beulke, Rn.458.

⁸⁰ Grünwald, JZ 1966, 489 ff.; Rogall, ZStW 1979, 1 ff.

บรรณานุกรม

ภาษาต่างประเทศ

- Albrecht, Hans-Jörg/ Dorsch, Claudia/ Krüpe-Gescher, Christiane. Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Freiburg: Max-Planck, 2003.
- Amelung, Knut. "Grundfragen der Verwertungsverbote bei beweissicheren Haussuchungen im Strafverfahren," NJW 1991, 2533.
- Bauer, Wolfram. "Ist die Kritik an der" Rechtskreistheorie " (methodisch) noch zu halten? – Ein Plädoyer für die Rechtskreistheorie – zugleich eine Erwiderung auf Hauf." NJW 1994, 2530.
- Bernsmann, Klaus. Anmerkung zum BGH, Urteil zum 16.02.1995. NStZ 1995, 512.
- Beulke, Werner. Strafprozessrecht. 14. Aufl. Karlsruhe: C.F.Müller, 2018.
- Bundesministerium der Justiz und für Verbraucherschutz (BMJV). Bericht der Expertenkommission zur effektiveren und praxistauglicheren Ausgestaltung des allgemeinen Strafverfahrens und des jugendgerichtlichen Verfahrens. Berlin: BMJV, 2005.
- Drucksache des deutschen Bundestages 16/5846 vom 27.06. 2007: Entwurf eines Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG. (zit. BT-Drs. 16/5846)

Drucksache des deutschen Bundestages 18/12785 vom 20.06.2017:
Beschlussempfehlung und Bericht des Ausschusses für
Recht und Verbraucherschutz (6. Ausschuss). (zit. BT-Drs.
18/12785)

Drucksache des deutschen Bundestages 18/5088 vom 09.06.2015:
Entwurf eines Gesetzes zur Einführung einer Speicherpflicht
und einer Höchstspeicherfrist für Verkehrsdaten. (zit. BT-Drs
. 18/5088)

Drucksache des deutschen Bundestages V/1880 vom 13.06.1967:
Entwurf eines Gesetzes zur Beschränkung des Briefs-,
Post- und Fernmeldegeheimnisse (Gesetz zur Artikel
10 Grundgesetz) (G10) (zit. BT-Drs. V/1880)

Drucksache des deutschen Bundestages VI/2722: Entwurf eines
dreizehnten Strafrechtsänderungsgesetzes (zit.
BT-Drs. VI/2722)

Eisenberg, Ulrich. Beweisrecht der StPO. 10. Aufl. München: C.H.Beck,
2017.

Fezer, Gerhard. "Grundfälle zum Verlesungs- und Verwertungsverbot
im Strafprozeß," JuS 1978, 104.

Gallas, Wilhelm. Der Schutz der Persönlichkeit im Entwurf eines
Strafgesetzbuchs, ZStW 1963, 16.

Geppert, Klaus. "Das Beweisverbot des § 252," Jura 1988, 305.

———. "Kontroll- und Förderungspflicht des Ermittlungsrichters,"
DRiZ 1992, 405.

Gössel, Karl Heinz. Löwe-Rosenberg Kommentar, Einleitung, Abschnitt L:
Beweisverbot. Berlin: De Gruyter, 2012.

Grote, Rainer, "Kommunkative Selbstbestimmung im Internet und Grundrechtsordnung," KritV 1999, 27.

Grünwald, Gerald. Beweisrecht der Strafprozessordnung. Baden-Baden: Nomos, 1993.

_____. Beweisverbote und Verwertungsverbote im Strafverfahren. JZ 1966, 489.

Hauck, Pierre: Heimliche Strafverfolgung und Schutz der Privatheit, Berlin: Mohr Siebeck, 2014.

Henkel, Heinrich. Strafverfahrensrecht: Ein Lehrbuch. 2. Aufl. Stuttgart: Kohlhammer, 1968.

Jäger, Christian. Beweisverwertung und Beweisverwertungsverbote im Strafprozess. München: C.H.Beck, 2003.

Kindhäuser, Urs. Strafrecht Besonderer Teil I, 3.Aufl. Baden-Baden: Nomos, 2007. (zit. Kindhäuser, BT I)

_____. Strafprozessrecht. 5. Aufl. Baden-Baden: Nomos, 2018. (zit. Kindhäuser, StPO)

Krüpe-Gescher, Kristiane. Die Überwachung der Telekommunikation nach den §§ 100a, 100b StPO in der Rechtspraxis. Freiburg: Max-Plank-Institut, 2005.

Küpper, Georg. Anmerkung zum BGH, Urteil zum 16.02.1995, JR 1996, 214.

Meyer-Goßner, Lutz/ Schmitt, Bertram. Strafprozessordnung. 61. Aufl. München: C.H. Beck, 2018.

Neuhaus, Ralf. Die strafprozessuale Überwachung der Telekommunikation. in: FS-Rieß. Berlin: De Gruyter, 2002.

- Niehaus, Holger. Katalogsysteme als Beschränkungen strafprozessualer Eingriffsbefugnisse, Berlin, 2001, 57.
- Paulus, Rainer. KMR – Kommentar zur Strafprozessordnung. München: Luchterhand, 1989.
- Rogall, Klaus. "Gegenwärtiger Stand und Entwicklungstendenzen der Lehre von den strafprozessualen Beweisverboten." ZStW 1979, 1.
- . "Hypothetische Ermittlungsverläufe im Strafprozess." NSTZ 1988, 385.
- Roxin, Claus/Schünemann, Bernd. Strafverfahrensrecht. 29. Aufl. München: C.H. Beck, 2017.
- Rudolphi, Hans Joachim. Strafprozess im Umbruch. ZRP 1976, 165.
- Schmidt, Eberhard. "Die Verletzung der Belehrungspflicht gemäß § 55 II StPO als Revisionsgrund." JZ 1958, 596.
- Schöneborn, Christian. "Die strafprozessuale Beweisverwertungsproblematik aus revisionsrechtlicher Sicht." GA 1975, 33.
- Schünemann, Bernd, Leipziger Kommentar Strafgesetzbuch. Berlin: De Gruyter, 2012.
- . "Der besondere Beitrag-Rundum betrachtet." JA 1972, 635.
- Störmer, Rainer. Der gerichtliche Prüfungsumfang bei Telefonüberwachungen – Beurteilungsspielraum bei Anordnungen nach § 100a StPO?, StV 1995, 653.
- Vassilaki, Irini. Die Überwachung des Fernmeldeverkehrs nach der Neufassung der §§ 100a, 100b StPO Erweiterung von staatlichen Grundrechtseingriffen?. JR 2000, 446.

Volk, Klaus/Engländer, Armin. Grundkurs StPO, 9. Aufl. München: C.H. Beck, 2018.

Welp, Jürgen. Die Entwicklung der Fernmeldeüberwachung in der BRD, Mangakis-FS, Athen, 1999, 813.

_____. Die strafprozessuale Überwachung des Post- und Fernmeldeverkehrs, Diss. Heidelberg, 1974.

Wessels, Johannes/Hettinger, Michael. Strafrecht Besonderer Teil 1, 34. Aufl. (München, C.F. Müller, 2010).



สถาบันพระปกเกล้า

ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา

อาคารรัฐประศาสนภักดี ชั้น 5 (โซนทิศใต้)

เลขที่ 120 หมู่ 3 ถนนแจ้งวัฒนะ

แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210

โทรศัพท์ 02-141-9567-70 โทรสาร 02-143-8175

www.kpi.ac.th



การให้รัฐเข้าถึงและได้มาซึ่งข้อมูลส่วนบุคคล
สื่อสารถึงกันในสหพันธรัฐเยอรมนี

ISBN : 978-616-476-046-2