

การคุ้มครองข้อมูลส่วนบุคคล: ประสบการณ์เยอรมัน¹

นคร เสรีรักษ์²

บทนำ

สังคมการเมืองไทยมีการเปลี่ยนแปลงอย่างมากในทศวรรษที่ผ่านมาทั้งทางด้านเศรษฐกิจ การเมืองและสังคม ส่วนหนึ่งเป็นผลมาจากการเปลี่ยนแปลงและพัฒนาการในบริบทสังคมโลก ซึ่งพัฒนาในลักษณะไร้พรมแดน รัฐต่างๆ มีการเรียนรู้ติดต่อสื่อสารเชื่อมโยงกันได้อย่างไร้ขีดจำกัด สังคมมีการพัฒนาไปสู่ความเป็นสังคมข้อมูลข่าวสารอย่างสมบูรณ์

ข้อมูลข่าวสารในปัจจุบันมีความสำคัญอย่างยิ่ง เนื่องจากสังคมสมัยใหม่เป็นสังคมแห่งการติดต่อสื่อสาร ข้อมูลข่าวสารจึงมีความสำคัญต่อการวางแผน ระบบการทำงานและการบริหารจัดการ การดำเนินกิจกรรมต่างๆ ไม่ว่าจะเป็นภาครัฐหรือเอกชน มีความจำเป็นต้องมีข้อมูลไว้ในครอบครองไว้ให้ได้มากที่สุด ซึ่งในข้อมูลข่าวสารจำนวนมากมายนานัปการที่มีการครอบครองแลกเปลี่ยนหรือแย่งชิงแข่งขันกันครอบครองนี้ มีข้อมูลข่าวสารส่วนหนึ่งเป็นข้อมูลส่วนบุคคล ปัญหาการละเมิดความเป็นส่วนตัวในข้อมูลส่วนบุคคลกำลังแพร่ขยายไปทั่วทุกมุมโลก จะมากบ้างน้อยบ้างแตกต่างกันไป ซึ่งดูเหมือนว่าเงื่อนไขของความรุนแรงของปัญหาจะขึ้นอยู่กับว่าสังคมนั้นมีความเจริญก้าวหน้าทางเทคโนโลยีมากน้อยเพียงใด เพราะเป็นที่ยอมรับกันว่าแรงกระตุ้นสำคัญที่ทำให้เกิดบรรทัดฐานนี้ก็เพราะความเจริญก้าวหน้าของเทคโนโลยีที่ส่งผลกระทบในทางลบต่อความเป็นส่วนตัวของบุคคล ข้อมูลส่วนบุคคลถูกเข้าถึงและเผยแพร่อย่างง่ายดายจากเทคโนโลยีเหล่านั้น บรรทัดฐานในประมวลกฎหมายในประเทศที่ใช้ระบบซีวิลลอว์ หลักกฎหมายในคอมมอนลอว์ หรือในกฎหมายเฉพาะเรื่อง ต่างไม่สามารถบังคับใช้ได้เพียงพอ และไม่ครอบคลุมสถานการณ์ที่มีเทคโนโลยีเข้ามาเกี่ยวข้อง ดังนั้น จึงมีความจำเป็นในการมีกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลขึ้น

¹บทความนี้เป็นส่วนหนึ่งของการวิจัยเรื่องคุ้มครองข้อมูลส่วนบุคคลของประเทศสหพันธ์สาธารณรัฐเยอรมนี ซึ่งเป็นการประมวลผลการสัมภาษณ์เจ้าหน้าที่ระดับสูง และผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลของเยอรมัน คือ Dr. Alexander Dix (Brandenburg Data Protection Commissioner) Prof. Dr. Hansjürgen Garstka (Berlin Data Protection Commissioner) Dr. Thilo Weichert (Schleswig-Holstein Data Protection Deputy Commissioner) และ Prof. Dr. Herbert Burkert (Data Protection Expert) และสำเร็จลงภายใต้การแนะนำของ Prof. Dr. Spiros Simitis และ ศศ.ดร. กิตติศักดิ์ ปรกติ ซึ่งผู้เขียนขอขอบคุณไว้ ณ ที่นี้

²PhD (ธรรมศาสตร์), Master of Policy Science (Saitama University), ร.ม. (ธรรมศาสตร์), ร.บ. (ธรรมศาสตร์)

ปัจจุบันประเทศไทยมีการคุ้มครองข้อมูลส่วนบุคคลโดยบทบัญญัติของพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. 2540 ซึ่งมีผลบังคับใช้ตั้งแต่เดือนธันวาคม 2540 เป็นต้นมา

หลักการของกฎหมายข้อมูลข่าวสารเป็นการประกันสิทธิแก่ประชาชน ในการเข้าถึงข้อมูลข่าวสารในครอบครองของหน่วยราชการ ภายใต้หลักที่ว่า "รัฐรู้อะไร ประชาชนรู้เท่านั้น" และข้อมูลราชการจะต้อง "เปิดเผยเป็นหลัก ปกปิดเป็นข้อยกเว้น"³ ขณะเดียวกันก็มีบทบัญญัติสำคัญในการคุ้มครองข้อมูลส่วนบุคคล ซึ่งถือว่าเป็นครั้งแรกในประเทศไทย ที่มีกฎหมายที่เป็นหลักประกันสิทธิความเป็นอยู่ส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล (Privacy and Personal Data Protection) สังคมและประชาชนได้ให้ความสนใจและตื่นตัวในกฎหมายข้อมูลข่าวสารนี้มาก อย่างไรก็ตาม ความรู้ความเข้าใจและองค์ความรู้ในเรื่องสิทธิรับรู้ข้อมูลข่าวสาร (Freedom of Information) และในเรื่องการคุ้มครองความเป็นส่วนตัวในข้อมูลและข้อมูลส่วนบุคคล (Informational Privacy and Personal Data Protection) ยังมีค่อนข้างจำกัด

วิชาการหรือองค์ความรู้เกี่ยวกับ "สิทธิที่จะรู้" ยังเป็นเรื่องที่ใหม่มากต่อสังคมไทย และจำเป็นต้องพัฒนาและสร้างเสริมความรู้แก่สังคมทั้งในส่วนเจ้าหน้าที่ของรัฐและประชาชนผู้ใช้สิทธิตามกฎหมาย ขณะเดียวกัน การปฏิบัติตามกฎหมายและการนโยบายนโยบายไปปฏิบัติโดยเฉพาะในเรื่องของ "ข้อมูลส่วนบุคคล" ซึ่งตามกฎหมายฉบับนี้ครอบคลุมเพียงข้อมูลส่วนบุคคลในส่วนที่อยู่ในครอบครองของรัฐ แต่ยังไม่ครอบคลุมถึงข้อมูลที่อยู่ในครอบครองขององค์กรธุรกิจและภาคเอกชน นอกจากนี้การคุ้มครองข้อมูลส่วนบุคคลยังเป็นประเด็นสำคัญในมิติความสัมพันธ์ระหว่างประเทศ เพราะในบางประเทศ เช่น กลุ่มประเทศในสหภาพยุโรป มีการออกข้อบังคับว่าด้วยการถ่ายทอดข้อมูล โดยจะไม่อนุญาตให้มีการส่งข้อมูลส่วนบุคคลให้ หากประเทศนั้นไม่มีกฎหมาย หรือมาตรการที่จะคุ้มครองข้อมูลส่วนบุคคลในมาตรฐานที่ยอมรับได้

เนื่องจากการคุ้มครองข้อมูลส่วนบุคคลยังเป็นองค์ความรู้ที่เพิ่งเริ่มต้นพัฒนาขึ้นในสังคมไทย ขณะที่ในต่างประเทศได้ผ่านประสบการณ์บังคับใช้กฎหมายและมาตรการต่างๆ เพื่อปกป้องคุ้มครองข้อมูลส่วนบุคคลมายาวนานกว่า ดังนั้นการศึกษามาตรการคุ้มครองข้อมูลส่วนบุคคลในประเทศที่มีพัฒนาการมาก่อน ย่อมจะช่วยให้สามารถทำการวิเคราะห์ และสังเคราะห์ข้อเสนอแนะเพื่อปรับใช้กับสถานการณ์ของประเทศไทยได้อย่างเหมาะสม ผู้เขียนได้ให้ความสนใจในกรณีของประเทศเยอรมันเป็นพิเศษ เพราะเป็นประเทศที่ใช้ระบบประมวลกฎหมาย เช่นเดียวกับประเทศไทย โดยเฉพาะอย่างยิ่งเป็นประเทศแรกในโลกที่มีกฎหมายคุ้มครองข้อมูล

³ นคร เสรีรักษ์, "สิทธิที่จะรู้ข้อมูลราชการ," กรุงเทพธุรกิจ (21 ตุลาคม 2542): 15.

ส่วนบุคคล และมีโครงสร้างการบังคับใช้กฎหมายในเรื่องนี้อย่างมีประสิทธิภาพ เป็นที่ยอมรับในระดับนานาชาติว่าเป็นต้นแบบของการคุ้มครองข้อมูลส่วนบุคคล

1. การคุ้มครองข้อมูลส่วนบุคคลในเยอรมัน

การคุ้มครองข้อมูลส่วนบุคคลของประเทศสหพันธ์สาธารณรัฐเยอรมนี อยู่ภายใต้บทบัญญัติของรัฐธรรมนูญ (German Constitution) ซึ่งเป็นกรอบการคุ้มครองที่สำคัญ ข้อมูลส่วนบุคคลได้รับความคุ้มครองโดยตรงจากบทบัญญัติของรัฐธรรมนูญ ซึ่งห้ามมิให้มีการเข้าไปแทรกแซงในสิทธิส่วนบุคคล เช่น ในกรณีที่มีข้อมูลนั้นเกี่ยวกับสิทธิขั้นพื้นฐานของบุคคลอื่นหรือของบุคคลที่สาม โดยในกฎหมายพื้นฐานฉบับนี้ (Basic Law or Grundgesetz) ได้ให้ความคุ้มครองความเป็นส่วนตัวของบุคคล ได้แก่ จดหมาย (letter) หรือวัตถุทางไปรษณีย์ (post) และการติดต่อสื่อสาร ทั้งนี้ การจำกัดความเป็นส่วนตัวดังกล่าวอาจทำได้ภายใต้บทบัญญัติของกฎหมายเท่านั้น⁴

กฎหมายของประเทศสหพันธ์สาธารณรัฐเยอรมนีที่เกี่ยวข้องกับเรื่องข้อมูลข่าวสารมีอยู่ 2 ฉบับ⁵ คือ “กฎหมายวิธีปฏิบัติราชการทางปกครอง” (Verwaltungsverfahrensgesetz - VwVfG) และ “กฎหมายว่าด้วยการคุ้มครองข้อมูล” (Bundesdatenschutzgesetz - BDSG 1)

กฎหมายวิธีปฏิบัติราชการทางปกครอง (VwVfG) ได้กำหนดเกี่ยวกับการเปิดเผยข้อมูลส่วนบุคคล โดยได้บัญญัติไว้ในมาตรา 30 ว่า “คู่กรณีมีสิทธิเรียกร้องไม่ให้เจ้าหน้าที่ของรัฐเปิดเผยความลับซึ่งอยู่ในขอบเขตส่วนบุคคล รวมทั้งข้อมูลอันเป็นความลับในทางธุรกิจได้”

2. พัฒนาการของกฎหมายคุ้มครองข้อมูลส่วนบุคคล

กฎหมายคุ้มครองข้อมูลในประเทศสหพันธ์สาธารณรัฐเยอรมนีเกิดขึ้นเป็นครั้งแรกเป็นกฎหมายระดับมลรัฐ (State Law) โดยเกิดขึ้นในรัฐเฮสเซน (Hessen) ในปี 1970 ซึ่งถือว่าเป็น

⁴ Grundgesetz “Basic Law,” (German Constitution) (May 23, 1949-Last amended August 31, 1990; English translation) Article 10 (Privacy of letters, posts, and telecommunications; amended 24 June 1968).

⁵ “เอกสารบันทึกหารือข้อกฎหมายกรณีการเปิดเผยข้อมูลข่าวสารที่เกี่ยวกับเอกสารการสอบ,” กฎหมายปกครอง, เมษายน 2543.

กฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับแรกของโลก หลังจากนั้น ในปี 1977 จึงได้มีการตรากฎหมายในระดับประเทศ (Federal Data Protection Act) ซึ่งกฎหมายฉบับนี้ได้มีการทบทวนและแก้ไขในปี ค.ศ.1990 และ 1994 และ 1997 ตามลำดับ⁶ ในปี ค.ศ.2001 ได้มีการทบทวนกฎหมายนี้อีกครั้งเพื่อให้เป็นไปตามแนวทางของข้อบังคับสหภาพยุโรป⁷ และการทบทวนแก้ไขครั้งสุดท้ายในปี 2002

"กฎหมายว่าด้วยการคุ้มครองข้อมูล" (BDSG) มีวัตถุประสงค์เพื่อคุ้มครองข้อมูลส่วนบุคคล โดยครอบคลุม การเก็บรวบรวม การประมวลผล และการใช้ ทั้งข้อมูลส่วนบุคคลที่ใช้โดยหน่วยงานของรัฐและข้อมูลส่วนบุคคลที่หน่วยงานภาคเอกชนมีไว้ เพื่อวัตถุประสงค์ในทางอาชีพหรือในทางธุรกิจ สำหรับข้อมูลส่วนบุคคลที่ใช้ประโยชน์โดยหน่วยงานของรัฐ หรือข้อมูลส่วนบุคคลที่หน่วยงานภาคเอกชนมีไว้ เพื่อวัตถุประสงค์ในทางอาชีพหรือในทางธุรกิจนั้น การใช้ประโยชน์จากข้อมูลส่วนบุคคลดังกล่าวทำได้เฉพาะเมื่อกฎหมายนี้หรือบทบัญญัติของกฎหมายอื่นอนุญาตให้กระทำได้ หรือเท่าที่บุคคลนั้นได้ให้ความยินยอมถ้าได้มีการขอความยินยอมจากผู้ที่เป็นเจ้าของข้อมูล ในกรณีนี้จะต้องกล่าวถึงวัตถุประสงค์ของการเก็บข้อมูลนั้นด้วย (มาตรา 4 (1))

กฎหมายคุ้มครองข้อมูลส่วนบุคคล (Data Protection Act) ของประเทศสหพันธ์สาธารณรัฐเยอรมนี ตั้งอยู่บนหลักการพื้นฐานในการคุ้มครอง "สิทธิของปัจเจกบุคคลในการกำหนดหรือตัดสินใจเกี่ยวกับการใช้หรือการดำเนินการใดๆ ที่เกี่ยวกับข้อมูลส่วนตัวของบุคคล" นั่นคือหลักการที่ว่า "บุคคลเป็นเจ้าของหรือผู้ควบคุมข้อมูลของตนเอง" นั่นเอง โดยมีกรณียกเว้นเท่านั้นที่บุคคลจำเป็นต้องเปิดเผยข้อมูลส่วนบุคคลเพื่อประโยชน์ส่วนรวม แต่หน่วยงานที่จะเก็บรวบรวมข้อมูลดังกล่าวต้องดำเนินการโดยน้อยที่สุดและเท่าที่กำหนดวัตถุประสงค์ไว้อย่างชัดเจนเท่านั้น และจะนำไปใช้เพื่อวัตถุประสงค์อื่นนอกเหนือจากที่กำหนดไว้ไม่ได้ นอกจากนี้บุคคลมีสิทธิที่จะได้รับรู้ว่าหน่วยงานมีการจัดเก็บและประมวลผลข้อมูลส่วนบุคคลของเขา และหากสงสัยว่ามี การดำเนินการใช้ข้อมูลของเขาโดยไม่ถูกกฎหมาย ก็สามารถแจ้งให้ผู้ตรวจการด้านการคุ้มครองข้อมูล (Data Protection Commissioner) ตรวจสอบแก้ไขให้ได้

กฎหมายว่าด้วยการคุ้มครองข้อมูล (BDSG) ได้ให้คำนิยามเฉพาะคำว่า "ข้อมูลส่วนบุคคล" (Personenbezogene Daten) ไว้ในมาตรา 3 ว่าหมายถึง "ข้อมูลอันใดอันหนึ่ง ที่เกี่ยวกับ

⁶"Federal Act on Data Protection ("BDSG") January 27, 1977 (Bundesgesetzblatt, Part I, No 7, February 1, 1977), Amended in 1990, <<http://www.datenschutz-berlin.de/gesetze/bdsg/bdsgeng.htm>>.

⁷*Ibid.*

เรื่องส่วนบุคคลของบุคคลธรรมดาบุคคลใดบุคคลหนึ่ง หรือของบุคคลธรรมดาที่อาจจะบ่งตัวได้" นอกจากนี้ ความหมายของ "ข้อมูลส่วนบุคคล" ตามมาตรา 30 VwVG หมายความว่ารวมถึงข้อมูลส่วนบุคคลอื่นๆ เช่น ข้อมูลส่วนบุคคล ข้อมูลเกี่ยวกับเรื่องความสัมพันธ์ภายในครอบครัว ข้อมูลเกี่ยวกับเรื่องทรัพย์สินและภาษีของบุคคล ข้อมูลเกี่ยวกับความลับในทางธุรกิจต่างๆ ฯลฯ

ประเทศสหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศหนึ่งที่ประสบความสำเร็จมาก ในเรื่อง การปฏิบัติงานของผู้ตรวจการด้านการคุ้มครองข้อมูลแห่งสหพันธ์รัฐ (Federal Data Protection Commissioner/ Bundesbeauftragter für den Datenschutz or FDPC) ซึ่งเป็นองค์กรอิสระของ รัฐและเป็นองค์กรผู้เชี่ยวชาญตามกฎหมายนี้ อำนาจหน้าที่ของผู้ตรวจการฯ มีดังนี้

1. ตรวจสอบดูแลการคุ้มครองการเก็บ การใช้ หรือการประมวลผลข้อมูล ของผู้ควบคุม ข้อมูล (Data Controller) นอกจากนี้ ยังมีอำนาจในการตรวจสอบดูแลเหนือองค์กร ผู้ประกอบวิชาชีพ หน่วยงานพิเศษในการรักษาความลับของราชการ (special official secrecy) โดยเฉพาะอย่างยิ่งข้อมูลที่เป็นความลับภายใต้บทบัญญัติประมวลกฎหมายภาษีอากร (Tax Code)

2. รับเรื่องร้องเรียนและสอบสวนคำร้องเรียน
3. ให้คำแนะนำต่อคณะรัฐมนตรีและองค์กรอื่นๆ ของรัฐ
4. จัดทำรายงานประจำปี¹⁰

ผู้ตรวจการด้านการคุ้มครองข้อมูล (ผู้ตรวจการฯ) มีวาระการดำรงตำแหน่ง 5 ปี และสามารถอยู่ในตำแหน่ง 2 วาระ ภารกิจหลักของผู้ตรวจการฯ คือการแก้ไขปัญหาข้อร้องเรียนของ ประชาชนในกรณีที่หน่วยงานของรัฐดำเนินการเกี่ยวข้องกับข้อมูลของบุคคล ผู้ตรวจการฯ มีสิทธิที่จะไม่เปิดเผยข้อมูลใดๆ ของผู้ตรวจการฯ แก่บุคคลที่สาม จึงเป็นการคุ้มครองประชาชนให้สามารถเปิดเผยข้อมูลแก่ผู้ตรวจการฯ ซึ่งถือเป็นผู้คุ้มครองข้อมูลชั้นสูงสุด (Supreme Data Protector) อย่างเต็มที่ ผู้ตรวจการฯ จะเสนอรายงานผลการดำเนินการต่อรัฐสภาทุก 2 ปี ซึ่งกระบวนการ

⁸ <<http://www.bfd.bund.de>>.

“มีผู้ให้ความหมายของคำว่า Data Protection Commissioner ไว้หลากหลาย เช่น กรรมการคุ้มครองข้อมูล เลขานุการคุ้มครองข้อมูล สำหรับในที่นี้ผู้เขียนเลือกใช้คำว่า ผู้ตรวจการด้านการคุ้มครองข้อมูล

¹⁰ “The duties of the Federal Data Protection Commissioner (in English),” <http://www.bfd.bund.de/information/datprotec_en.html>.

นำเสนอผลการตรวจสอบ ตลอดจนข้อเสนอเพื่อการปรับปรุงต่อรัฐสภา นับว่าเป็นกลไกที่ดีที่สุดใน การแสดงความเห็นสาธารณะ (Public Opinion) ในสังคมประชาธิปไตย

ประชาชนเยอรมันจึงสามารถร้องเรียนหรือขอความคุ้มครองจากผู้ตรวจการฯ ซึ่งมา จากการเลือกตั้งโดยรัฐสภา อันเป็นการรับรองความชอบธรรมของผู้ตรวจการฯ ตามหลักการ ประชาธิปไตย (Democratic Legitimacy) และเป็นการยืนยันอย่างชัดเจนของความเป็นอิสระของ ผู้ตรวจการฯ ว่าสามารถเป็นที่พึ่งของประชาชนในการเผชิญหน้ากับการเก็บข้อมูลของระบบ ราชการ (Automated Bureaucracy)

การคุ้มครองข้อมูลส่วนบุคคลที่ใช้โดยหน่วยงานของรัฐ ในกรณีที่บุคคลผู้เป็นเจ้าของ ข้อมูลเห็นว่า การใช้ข้อมูลที่เกี่ยวข้องกับตนโดยหน่วยงานของรัฐเป็นการละเมิดสิทธิของตน ก็อาจ ได้แจ้งการใช้ข้อมูลของหน่วยงานของรัฐนั้นต่อผู้ตรวจการฯ ได้ (มาตรา 21) และหากผู้ตรวจการฯ วินิจฉัยขัดกับบทบัญญัติของกฎหมาย บุคคลนั้นอาจอุทธรณ์เรื่องไปยังรัฐมนตรีได้ (มาตรา 25) การโต้แย้งคำวินิจฉัยของรัฐมนตรีอาจกระทำได้โดยการเสนอเรื่องไปยังศาลปกครอง

การคุ้มครองข้อมูลส่วนบุคคลที่อยู่ในความครอบครองของหน่วยงานภาคเอกชน ใน กรณีที่หน่วยงานภาคเอกชน มีข้อมูลส่วนบุคคลไว้เพื่อวัตถุประสงค์ในทางอาชีพ หรือในทางธุรกิจ ให้หน่วยงานของเอกชนนั้นแต่งตั้งพนักงานของหน่วยงานนั้นที่มีความรู้ความสามารถในด้านการ เก็บรักษาข้อมูลคนหนึ่ง ทำหน้าที่ในการคุ้มครองข้อมูล (Beauftragte fuer Datenschutz) พนักงานผู้ทำหน้าที่ดูแลข้อมูลของหน่วยงานดังกล่าวทำหน้าที่ภายใต้การดูแลของ "เจ้าหน้าที่ ตรวจสอบของสหพันธ์" (Aufsichtsbene) (มาตรา 36 และมาตรา 37) ในกรณีที่ผู้เป็นเจ้าของ ข้อมูลเห็นว่า การใช้ข้อมูลนั้นกระทบสิทธิของตน บุคคลนั้นอาจร้องเรียนไปยัง "เจ้าหน้าที่ตรวจสอบ ของสหพันธ์" ได้ (มาตรา 38) และคำวินิจฉัยของ "เจ้าหน้าที่ตรวจสอบของสหพันธ์" ย่อมถูกโต้แย้ง ไปยังศาลปกครองได้ เช่นเดียวกับคำวินิจฉัยของรัฐมนตรีดังกล่าวข้างต้น

นับจากมีการแก้ไขปรับปรุงกฎหมายฉบับนี้ได้มีการเพิ่มเติมหลายประเด็น เช่น การส่ง ข้อมูลที่เกี่ยวข้องกับบุคคลระหว่างประเทศ การสำรวจตรวจตราโดยกล้องวิดีโอ (Video surveillance) การปิดบังชื่อ (anonymization) การใช้นามแฝง (pseudonymization) การจัดทำบัตรประจำตัวใน ลักษณะที่มีการเก็บข้อมูลส่วนบุคคล (smart cards) และเกี่ยวกับการเก็บสะสมข้อมูลข่าวสาร ประเภทที่เป็นเรื่องเฉพาะตัว ซึ่งในข้อมูลเหล่านี้ กฎหมายอนุญาตให้เจ้าของข้อมูลใช้สิทธิที่จะ ปฏิเสธ และได้ทำให้เกิดระบบลงทะเบียน ซึ่งบุคคลหรือองค์กรที่มีการเก็บข้อมูลต้องลงทะเบียนต่อ Data Protection Authorities (DPAs) ซึ่งเป็นแนวทางที่ประเทศในภาคพื้นยุโรปมักใช้ระบบจด ทะเบียนกับหน่วยงานของรัฐที่ตั้งขึ้น โดยอยู่บนหลักการที่ต้องขอความยินยอมจากเจ้าของข้อมูล

ในการเก็บรวบรวม ประมวลผล หรือการเปิดเผยข้อมูล และหลักการที่เจ้าของข้อมูลต้องได้รับการแจ้งถึงผลที่จะได้รับ หากมีการเก็บสะสมหรือมีการใช้ข้อมูลดังกล่าว

นอกจากนี้กฎหมายระดับสหพันธรัฐที่สำคัญได้แก่กฎหมาย G-10 (แก้ไขเพิ่มเติม ปี ค.ศ.2001)¹¹ ซึ่งเป็นบทบัญญัติที่กำหนดให้มีการจำกัดการรักษาความลับของการติดต่อสื่อสารบางประการ ซึ่งภายใต้กฎหมายนี้กำหนดให้ผู้ให้บริการโทรศัพท์ต้องอยู่ภายใต้บังคับของกฎหมายในการตรวจสอบดูแล การควบคุมข้อมูลการติดต่อสื่อสารเช่นเดียวกับข้อมูลทั่วไป นอกจากนี้ผู้ตรวจการด้านการคุ้มครองข้อมูล ยังมีนโยบายที่จะพยายามให้ผู้ให้บริการอินเทอร์เน็ต (Internet Service Providers : ISP) มีมาตรการในการคุ้มครองความเป็นส่วนตัว เพื่อใช้ในการเก็บข้อมูลของผู้เข้าใช้บริการ รวมถึงการตรวจสอบอีเมล (e-mail) และการเก็บข้อมูลที่เกี่ยวข้อง¹² และในเดือนตุลาคม 2001 รัฐบาลได้ผ่านกฎหมายเกี่ยวกับการควบคุมบริษัทที่มีการจัดและติดตั้งระบบการติดต่อสื่อสารแบบไร้สาย¹³ ซึ่งการดักฟังทางโทรศัพท์ที่อยู่ภายใต้กฎหมาย G-10 ซึ่งกำหนดให้อยู่ภายใต้การพิจารณาของศาล

หลังจากที่รัฐบาลอนุญาตให้เจ้าหน้าที่ของรัฐด้านการข่าว (Intelligence Service) มีอำนาจดักฟังโทรศัพท์ได้ ในกรณีที่มีวัตถุประสงค์เพื่อเป็นการป้องกันการก่อการร้าย (terrorism) การค้ายาเสพติด และการค้าอาวุธที่ผิดกฎหมาย ปรากฏว่ามีการดักฟังโทรศัพท์เกิดขึ้นอย่างกว้างขวาง ขณะเดียวกัน การตรวจสอบการใช้โทรศัพท์ก็มีเพิ่มมากขึ้น ทั้งการดักฟังโทรศัพท์ธรรมดาและโทรศัพท์มือถือเกิดขึ้นทั่วไป (Grosser Lauschangriff or Big Eavesdropping Attack)¹⁴ ซึ่งการกระทำเหล่านี้ถูกวิพากษ์วิจารณ์ทั่วไปว่าเป็นการละเมิดความเป็นส่วนตัว และเป็นการทำลายศักดิ์ศรีความเป็นมนุษย์ ในปี 2001 จึงได้ออกกฎหมายว่าด้วยข้อมูลการติดต่อสื่อสาร (Telecommunication connection data) สำหรับใช้บังคับในการสืบสวนคดีอาญาร้ายแรง กฎหมายมีผลเมื่อเดือนมกราคม 2002 กำหนดให้ผู้ให้บริการการติดต่อสื่อสารเปิดเผย

¹¹"Federal Republic of Germany,"

<<http://pi.gn.apc.org/survey/phr2003/countries/germany.htm>>.

¹²*Ibid.*

¹³"Telekommunikations-überwachungsverordnung - TKÜV," January 22, 2002, BGBl. I Nr. 5, 458, <<http://217.160.60.235/BGBL/bgbl1f/bgbl102005s458.pdf>>; Steve Gold, "German Carriers Told To Install Cyber-Snooping Tech," Newsbytes, October 25, 2001.

¹⁴*supra* note 7.

ข้อมูล เช่น เวลาและระยะเวลาในการใช้โทรศัพท์ และหมายเลขโทรศัพท์เพื่อการสืบสวนคดีอาชญากรรมร้ายแรง¹⁵ อย่างไรก็ตาม ในปัจจุบันนี้พบว่าการดักฟังโทรศัพท์กว่า 75% เป็นการกระทำที่ไม่ชอบด้วยกฎหมาย ส่วนใหญ่ไม่ได้มีการแจ้งแก่เจ้าของโทรศัพท์ นอกจากนี้ มีกฎหมาย Telecommunications Carriers Data Protection Ordinance of 1996 แก้ไขเพิ่มเติม ปี 2000 คุ้มครองความเป็นส่วนตัวของบุคคลในข้อมูลในการติดต่อสื่อสาร¹⁶

การกระทำความผิดกล่าวทำให้รัฐต้องกลับมาทบทวนการกระทำของตน ซึ่งต่อมารัฐสภาได้เปลี่ยนแปลงบทบัญญัติรัฐธรรมนูญในบางมาตรา (มาตรา 13) เกี่ยวกับการใช้อำนาจของเจ้าหน้าที่ตำรวจ ในการติดตั้งเครื่องดักฟังการสนทนาในบ้านของบุคคลซึ่งจะทำได้โดยคำสั่งศาล การเปลี่ยนแปลงดังกล่าวนำมาซึ่งการออกกฎหมาย Law for the Enhancement of the Fight Against Organized Crime ซึ่งการออกกฎหมายดังกล่าว ทำให้เจ้าหน้าที่ตำรวจ (Bundeskriminalamt or Federal Police) สามารถสร้างระบบฐานข้อมูลในระดับชาติ ในการจัดเก็บข้อมูลทางพันธุกรรมที่เกี่ยวข้องกับการสืบสวนในคดีอาชญากรรมและข้อมูลของผู้กระทำความผิด หนึ่งเดือนต่อมา ได้มีการออกกฎหมายให้ตำรวจตรวจคนเข้าเมือง (Bundesgrenzschutz หรือ Border Protection Forces) ซึ่งเป็นตำรวจที่รับผิดชอบดูแลความปลอดภัยบนรถไฟและในสถานีรถไฟ ให้มีอำนาจในการตรวจบัตรประจำตัว และหีบห่อสัมภาระของบุคคล¹⁷

นอกจากนี้ยังมีโครงการ Data Protection in Teleservices (DASIT) ซึ่งเป็นโครงการพัฒนา software เพื่อใช้ให้เหมาะสมกับการคุ้มครองข้อมูลในเครื่องคอมพิวเตอร์ ซึ่งมีเป้าหมายให้มีการติดตั้งในร้านที่ให้บริการอินเทอร์เน็ตเพื่อคุ้มครองความปลอดภัยในข้อมูลของลูกค้า

เมื่อวันที่ 26 กันยายน 2001 รัฐบาลสหพันธ์รัฐ ได้เสนอให้มีการออกกฎหมายว่าด้วยการเข้าถึงข้อมูลข่าวสาร (Freedom of Information Act) ในระดับสหพันธ์รัฐ ซึ่งอนุญาตให้ประชาชนเข้าถึงข้อมูลข่าวสารของรัฐได้ อย่างไรก็ตามในบางรัฐ (Länder) มีการออกกฎหมายว่า

¹⁵"Federal Bulletin, BGBl I 2001, 3879, archived at <http://217.160.60.235/BGBl/bgbl1f/b101073f.pdf>.

¹⁶Telecommunications Carriers Data Protection Ordinance ("TDSV") of July 12, 1996 (Federal Law Gazette, I, 982), Federal Ministry of Posts and Telecommunications, <<http://www.datenschutz-berlin.de/gesetze/medien/tdsve.htm>>.

¹⁷"New Powers For The Border Police: Checks Anywhere At Any Time," Fortress Europe, FECL 56 (December 1998).

ด้วยการเข้าถึงข้อมูลข่าวสารของตนเอง ซึ่งอนุญาตให้ประชาชนเข้าถึงข้อมูลข่าวสารของรัฐและมีผู้ตรวจการฯ เป็นผู้บังคับให้เป็นไปตามกฎหมาย

ในประเทศสหพันธ์สาธารณรัฐเยอรมนี มีการออกกฎหมายใหม่ๆ มากมาย เพื่อรองรับวิวัฒนาการใหม่ๆ ทางวิทยาศาสตร์และเทคโนโลยี เช่น The Counterterrorism Act มีผลบังคับใช้เมื่อเดือนมกราคม ค.ศ.2002 ซึ่งเป็นหลักกฎหมายที่ถูกสร้างขึ้นเพื่อรองรับการใช้ลักษณะบ่งชี้ทางชีวภาพ (Biometric identification) ในหนังสือเดินทางและบัตรประจำตัวประชาชน หรือเรียกรวมว่า Biometric Identification Cards¹⁸ เช่น การใส่ลายพิมพ์นิ้วมือ หรือเทคโนโลยีที่ใช้ในการที่เฉพาะตัวบุคคลจากหน้าตาหรือม่านดวงตาซึ่งอาจจะมิขึ้นได้ในอนาคต ซึ่งจะทำให้หน่วยงานหลายแห่งสามารถใช้ข้อมูลที่อยู่ในหนังสือเดินทางและบัตรประจำตัวประชาชนดังกล่าวร่วมกันได้ง่ายยิ่งขึ้น ซึ่งประเด็นดังกล่าวนี้ได้รับความสนใจจากผู้ตรวจการฯ เป็นอย่างยิ่งเกี่ยวกับมาตรการในการรักษาความปลอดภัยในข้อมูลลักษณะบ่งชี้ทางชีวภาพนี้ นอกจากจะกังวลเรื่องความปลอดภัยแล้วยังกังวลเรื่องการนำไปใช้ เนื่องจากข้อมูลเหล่านี้เป็นข้อมูลเฉพาะตัวบุคคลอย่างแท้จริง การใช้จึงจะต้องใช้ในวัตถุประสงค์ที่เฉพาะเจาะจงเท่านั้น และต้องมีเครื่องมือในการตรวจสอบความถูกต้องเพื่อป้องกันการฉ้อฉลหรือการนำไปใช้ในทางที่ผิด ซึ่งจะทำให้เกิดความเสียหายต่อบุคคล

เมื่อปี 2000 เริ่มมีการใช้เทคโนโลยีใหม่คือ การติดตั้งเครื่องมืออิเล็กทรอนิกส์ในการเก็บค่าผ่านทางบนทางหลวง(National highways) โดยการติดตั้งระบบแจ้งตำแหน่ง (Global Positioning System) ที่ล้อรถ ซึ่งใช้ร่วมกับโทรศัพท์เคลื่อนที่ ซึ่งเทคโนโลยีดังกล่าวนี้ใช้เพื่อวัตถุประสงค์ในการเก็บเงินค่าผ่านทางเท่านั้น ข้อมูลทั้งหมดจะถูกลบเมื่อมีการจ่ายเงินค่าผ่านทางแล้ว เช่นเดียวกับการใช้เทคโนโลยี SMSI-Catcher เป็นระบบที่ใช้ติดตามร่องรอยบุคคลจากการใช้โทรศัพท์มือถือของบุคคลนั้น จากเทคโนโลยีดังกล่าวทำให้ผู้ตรวจการฯ ให้ความสนใจเกี่ยวกับปัญหาการละเมิดความเป็นส่วนตัวอย่างมาก อย่างไรก็ตาม ขณะนี้ปัญหาเกี่ยวกับกรณีดังกล่าวได้ถูกปรับใช้ในประมวลกฎหมายอาญา (Criminal Code : StPO)¹⁹

¹⁸"Federal Republic of Germany,"

<<http://pi.gn.apc.org/survey/phr2003/countries/germany.htm>>.

¹⁹"Federal Republic of Germany,"

<<http://pi.gn.apc.org/survey/phr2003/countries/germany.htm>>.

3. สถานภาพปัจจุบันของการคุ้มครองข้อมูล²⁰

ประเทศสหพันธ์สาธารณรัฐเยอรมนีเป็นประเทศแรกในโลก ที่มีการใช้กฎหมายคุ้มครองข้อมูล (Data Protection Law) ซึ่งนับถึงวันนี้ การปฏิบัติตามกฎหมายดังกล่าวผ่านมานานกว่า 30 ปี รูปแบบการคุ้มครองข้อมูลส่วนบุคคลของเยอรมัน ถือเป็นแบบฉบับ (Data Protection Model) ที่หลายฝ่ายยอมรับและให้ความสนใจ นอกเหนือจากการศึกษาตัวบทกฎหมายแล้ว การศึกษาทำความเข้าใจสถานการณ์ที่เป็นจริง (Reality) ของการปฏิบัตินโยบายมีความสำคัญไม่น้อยกว่ากัน

ผู้เขียนได้มีโอกาสพูดคุยแลกเปลี่ยนความคิดเห็นกับเจ้าหน้าที่ระดับสูง และผู้เชี่ยวชาญด้านการคุ้มครองข้อมูลของเยอรมัน คือ ดร. อเล็กซานเดอร์ ดิกส์ (Dr. Alexander Dix) ผู้ตรวจการด้านการคุ้มครองข้อมูลแห่งรัฐบรานเดนบวร์ก (Brandenburg Data Protection Commissioner) ศาสตราจารย์ ดร. ฮันส์เจอร์เกน การ์สคา (Prof. Dr. Hansjürgen Garstka) ผู้ตรวจการด้านการคุ้มครองข้อมูลแห่งนครเบอร์ลิน (Berlin Data Protection Commissioner) ดร. ทิลโล ไวแซร์ต (Dr. Thilo Weichert) รองผู้ตรวจการด้านการคุ้มครองข้อมูลแห่งเชลสวิค-โฮลสไตน์²¹ (Schleswig-Holstein Data Protection Deputy Commissioner) และ ศาสตราจารย์ ดร. แอแบร์ต บัวร์เคิร์ต (Prof. Dr. Herbert Burkert) ผู้เชี่ยวชาญด้านการคุ้มครองข้อมูล (Data Protection Expert) ซึ่งประเด็นการพูดคุยแสดงให้เห็นภาพปัจจุบันของการคุ้มครองข้อมูลส่วนบุคคลในประเทศสหพันธ์สาธารณรัฐเยอรมนี ดังนี้

3.1 ความตระหนักรู้ในเรื่องการคุ้มครองข้อมูล

1) ความตระหนักรู้ของสังคม

²⁰ สถานการณ์การคุ้มครองข้อมูลส่วนบุคคลในเยอรมันในส่วนนี้เป็นการสรุปจากการพูดคุยและสัมภาษณ์ ซึ่งดำเนินการในประเทศสหพันธ์สาธารณรัฐเยอรมนี ระหว่าง เดือน เมษายน-กรกฎาคม 2546. โดยได้รับการสนับสนุนจากสำนักงานคณะกรรมการส่งเสริมการวิจัย และ DAAD

²¹ ปัจจุบัน ดร. ทิลโล ไวแซร์ต ดำรงตำแหน่งผู้ตรวจการด้านการคุ้มครองข้อมูลแห่งเชลสวิค-โฮลสไตน์

ดิกส์ อธิบายว่า ประชาชนเยอรมันยังตื่นตัวค่อนข้างน้อยต่อความสำคัญของประเด็นความโปร่งใส และสิทธิรับรู้ข้อมูลข่าวสาร ทั้งนี้เนื่องจากวัฒนธรรมการบริหารแบบไม่เปิดเผย (Secrecy Administration Tradition) มีพัฒนาการมานานกว่า 150 ปี เอกสารราชการจะถูกเก็บเป็นความลับทั้งหมด และหากประชาชนต้องการตรวจสอบเอกสารดังกล่าวจะต้องอธิบายเหตุผล แต่ภายใต้หลักการสิทธิเข้าถึงข้อมูลข่าวสาร (Freedom of Information) มิใช่ประชาชนที่เป็นผู้ให้เหตุผลอีกต่อไป แต่เจ้าหน้าที่ของรัฐจะต้องเป็นผู้อธิบายเหตุผลว่าเหตุใดจึงเปิดเผยเอกสารให้ดูไม่ได้ ประเด็นนี้เป็นการเปลี่ยนแปลงทางวัฒนธรรมของระบบบริหารและปฏิบัติราชการ (Administrative Culture) ซึ่งทั้งประชาชนและเจ้าหน้าที่อยู่ระหว่างการปรับตัวให้รับต่อทัศนคติใหม่ดังกล่าว แต่ความตื่นตัวนับว่าช้าเมื่อเทียบกับอเมริกา ที่มีกฎหมายมานานกว่า 30 ปี อย่างไรก็ตาม การเปลี่ยนแปลงทัศนคติต้องดำเนินการอย่างค่อยเป็นค่อยไป

ในขณะที่ประเด็นการคุ้มครองข้อมูลส่วนบุคคล มีการพัฒนาการยาวนานกว่าร่วม 30 ปี จนนับว่ามีความรับรู้เรื่องนี้อย่างดี ทั้งในระดับจิตสำนึกสาธารณะ (Public Mind) และในระดับแนวคิดในการบริหาร (Administrative Concept) อย่างไรก็ตาม ยังคงมีปัญหาในการปฏิบัติอยู่บ้าง เช่น บางครั้งมีข้อสงสัยว่ารัฐจะสามารถก้าวล่วงสิทธิความเป็นส่วนตัวของบุคคลได้เพียงใด หรือจะยอมให้รัฐเก็บข้อมูลส่วนบุคคลได้หรือไม่เพียงใด และประเด็นความสัมพันธ์ระหว่างการคุ้มครองข้อมูลส่วนบุคคล (Data Protection) และสิทธิเข้าถึงข้อมูลข่าวสาร (Freedom of Information) ซึ่งในกรณีสิทธิเข้าถึงข้อมูลข่าวสาร จะไม่มีข้อยุ่งยากหากเป็นข้อมูลที่ไม่ใช่ข้อมูลส่วนบุคคล (Nonpersonal Data) แต่หากเป็นข้อมูลส่วนบุคคล จะต้องมีการพิจารณาซึ่งน้ำหนักระหว่างสิทธิส่วนบุคคล และประโยชน์สาธารณะว่าสิ่งใดมีความสำคัญกว่ากัน

เกี่ยวกับความตระหนักของผู้ของสังคมนั้น ไวชาร์ตเห็นว่ามีเพิ่มมากขึ้นในปัจจุบัน โดยเฉพาะในด้านการคุ้มครองข้อมูลในการ Online หรือ Internet เพราะประชาชนจะสนใจในเรื่องของการควบคุมข้อมูลสื่อสาร (Communication Data) ประชาชนจะลังเลและไม่แน่ใจในการใช้บริการผ่านอินเทอร์เน็ต หากไม่แน่ใจว่าจะเกิดอะไรขึ้นกับข้อมูลส่วนบุคคลของตนเอง ประชาชนต้องการความมั่นใจว่าจะปกป้องตัวเองได้อย่างไรในโลกอินเทอร์เน็ต

ในส่วนของความตื่นตัวในเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับสิทธิเข้าถึงข้อมูลข่าวสารนั้น ไวชาร์ตเห็นว่าเป็นสิ่งที่ดำเนินการไปโดยควบคู่กัน เช่น ในรัฐ 3 แห่ง คือ รัฐบรานเดนบวร์ก นอร์ทไรน์-เวสต์ฟาเลีย (Northrhine Westphalia) เชลซวิก โฮลสไตน์ และมหานครเบอร์ลิน สำนักงานผู้ตรวจการด้านการคุ้มครองข้อมูล รับผิดชอบงานกำกับดูแลกฎหมายทั้งสองฉบับนี้ งานส่งเสริมความตระหนักแก่ประชาชนจึงเกิดการควบคู่กันไปโดยไม่ขัดแย้ง รวมทั้งองค์กรทางการเมือง ประชาสังคมก็มีการเคลื่อนไหวในทั้งสองเรื่องไปพร้อมๆ กัน

ในเรื่องนี้ การ์สคาเห็นว่าการตื่นตัวและตระหนักรู้ของประชาชนมีมากขึ้น โดยผลของพัฒนาการในเรื่องอินเทอร์เน็ตทำให้ประชาชนจำนวนมากขึ้นเริ่มมองเห็นถึงปัญหา เนื่องจากพวกเขามีการเก็บข้อมูลส่วนบุคคลในอินเทอร์เน็ตจำนวนมาก ในขณะที่เขาไม่รู้ว่าข้อมูลจะถูกส่งไปที่ไหน ใครจะใช้ข้อมูลเหล่านี้ได้บ้าง เขาจะมั่นใจได้หรือไม่ในการแจ้งหมายเลขบัตรเครดิตในอินเทอร์เน็ต ใครจะเข้าถึงข้อมูลเหล่านี้ได้บ้าง ซึ่งหากไม่มีหลักประกันความปลอดภัยในการคุ้มครองข้อมูลส่วนบุคคล จะไม่มีผู้ใดเข้ามาใช้ระบบการพาณิชย์อิเล็กทรอนิกส์ (E-Commerce) รวมถึงรัฐบาลอิเล็กทรอนิกส์ (E-Government)

การ์สคาเห็นว่าการดำเนินการเรื่องสิทธิเข้าถึงข้อมูลข่าวสารและการคุ้มครองข้อมูลส่วนบุคคล จะต้องทำควบคู่กันไป โดยจะต้องสร้างสมดุลระหว่างสองสิ่งนี้ นั่นคือโดยหลักความโปร่งใสก็ต้องเปิดโอกาสให้ประชาชนสามารถเข้าถึงข้อมูลได้มากที่สุด แต่ในขณะที่โดยหลักสิทธิความเป็นส่วนตัวข้อมูลส่วนบุคคลจะต้องได้รับความคุ้มครองเต็มที่เช่นกัน และเขาเห็นว่าการบริหารกฎหมายทั้งสองฉบับโดยสำนักงานผู้ตรวจการฯ นั้นเหมาะสมแล้ว เขาเห็นว่าการมีผู้ตรวจการฯ สองคนจะทำให้สับสนและไม่มีประสิทธิภาพ

บัวร์เคิร์ทอธิบายว่ามีความตระหนักรู้ในเรื่องการคุ้มครองข้อมูลส่วนบุคคล ทั้งในฝ่ายราชการ ประชาชนและในภาคธุรกิจ แต่อย่างไรก็ตาม ในบางสถานการณ์ก็ทำให้มีการละเลยความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน เช่น ในบางสถานการณ์ทางการเมืองที่อ้างความจำเป็นเพื่อความมั่นคงของรัฐ ประชาชนก็อาจหลงลืมหรือละเลยความจำเป็นที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคล จึงจำเป็นต้องย้ำหรือกระตุ้นเตือนให้ประชาชนยังคงมีสำนึกในเรื่องนี้อย่างสม่ำเสมอ

บัวร์เคิร์ทอธิบายว่าภาคเอกชนซึ่งเข้าใจและตระหนักรู้ในเรื่องการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างดี แต่ในบางครั้งเมื่อต้องการเก็บรวบรวมหรือประมวลผลข้อมูลเพื่อผลประโยชน์ทางธุรกิจ ก็จะต้องมีการสอดส่องหรือกำกับมิให้มีการละเลยหลักการของการคุ้มครองข้อมูลส่วนบุคคล เช่นในกรณีที่ภาคธุรกิจพยายามรวบรวมข้อมูลจากการประกอบธุรกิจหรือการซื้อขายสินค้า จากนั้นจึงนำข้อมูลไปเก็บในคลังข้อมูล (Data Warehouse) เพื่อทำการประมวลเพื่อวิเคราะห์หาแบบแผนพฤติกรรมผู้บริโภค ซึ่งจะนำไปใช้ในการกำหนดยุทธศาสตร์ทางการตลาด ลักษณะดังกล่าวขัดกับหลักการคุ้มครองข้อมูลส่วนบุคคล ที่กำหนดให้การเก็บข้อมูลต้องมีวัตถุประสงค์ในการเก็บที่จำกัด และข้อมูลจะนำไปใช้ได้เฉพาะที่เป็นไปตามวัตถุประสงค์ที่แจ้งแก่เจ้าของข้อมูล ขณะที่เก็บข้อมูลเท่านั้น การนำข้อมูลมาเชื่อมโยงและประมวลผลดังกล่าวจึงไม่เป็นไปตามวัตถุประสงค์ที่ชี้แจงแก่เจ้าของข้อมูลในการจัดเก็บแต่ต้น

2) ความตระหนักรู้ในส่วนของเจ้าหน้าที่

ในส่วนของเจ้าหน้าที่ของสำนักงานผู้ตรวจการฯ บัณฑิตศิริอธิบายว่าอยู่ในเกณฑ์ที่มีประสิทธิภาพและมีความรู้ความเข้าใจในปรัชญาการคุ้มครองข้อมูลเป็นอย่างดี ข้อผิดพลาดที่เกิดขึ้นจะเป็นปัญหาในการบริหารจัดการมากกว่า เช่น เมื่อหน่วยงานจะเก็บข้อมูลส่วนบุคคลในเรื่องใดเรื่องหนึ่งซึ่งเป็นเรื่องใหม่ก็มักดำเนินการไปก่อน โดยไม่คำนึงถึงหลักปฏิบัติในเรื่องการคุ้มครองข้อมูล จากนั้นจึงมาพิจารณาหลักการในภายหลัง

ปัญหาในด้านวัฒนธรรมองค์กรก็มีส่วนทำให้การปฏิบัติงานของหน่วยงานละเลยหลักการคุ้มครองข้อมูลส่วนบุคคลเช่นกัน การสาคอธิบายว่า หน่วยงานตำรวจและองค์กรด้านความมั่นคงจะมีวัฒนธรรมองค์กรที่มุ่งเน้นและอ้างเหตุผลเพื่อการรักษาความมั่นคง และจะใช้ข้ออ้างนี้เพื่อให้ตนสามารถเก็บข้อมูลของประชาชนให้มากและนานที่สุดตามที่ตนต้องการ ซึ่งโดยที่จริงแล้ว การเก็บข้อมูลของตำรวจหรือหน่วยงานด้านความมั่นคงจะทำได้ก็ต่อเมื่อมีกฎหมายบัญญัติให้อำนาจเท่านั้น และต้องปฏิบัติโดยหลักแห่งความจำเป็น (Principle of Necessity) คือสามารถเก็บได้เท่าที่จำเป็นต่อภารกิจในการรักษาความมั่นคงเท่านั้น และต้องยึดหลักความปลอดภัย (Principle of Security) คือต้องทำลายข้อมูลที่ไม่ได้ประโยชน์ในเวลาที่เหมาะสม นอกจากนี้ หน่วยงานด้านสวัสดิการสังคม สาธารณสุข บริการสังคมหรือการประกันสังคม ก็มีการเก็บและใช้ข้อมูลส่วนบุคคล ที่เป็นข้อมูลที่เป็นเรื่องเฉพาะตัว (Sensitive Data) เพราะเมื่อประชาชนยื่นขอรับสวัสดิการดังกล่าว จะต้องแจ้งข้อมูลเกี่ยวกับสุขภาพ รายได้ สถานภาพครอบครัว ทำให้หน่วยงานดังกล่าวมีการเก็บข้อมูลเรื่องเฉพาะตัวไว้มหาศาล จึงต้องมีการออกกฎหมายมารองรับ

ในการแก้ไขปัญหาเมื่อมีการร้องเรียนเกี่ยวกับการล่วงละเมิดข้อมูลส่วนบุคคล ของประชาชน สำนักงานผู้ตรวจการฯ จะทำรายงานเปิดเผยต่อสาธารณะ และหน่วยงานจะต้องมาชี้แจงต่อสำนักงานผู้ตรวจการฯ ไวแซร์ตเห็นว่าการทำงานของสำนักงานผู้ตรวจการฯ จึงเน้นที่การเป็นหน่วยงานให้คำปรึกษา (Consulting Authority) มากกว่าการควบคุมหรือลงโทษ ยิ่งหน่วยงานเปิดกว้างสำหรับให้หน่วยงานมาปรึกษา หน่วยงานก็จะยิ่งให้ความยอมรับและรับฟังคำแนะนำของสำนักงาน ความสัมพันธ์ของหน่วยงานกับสำนักงานผู้ตรวจการฯ ของเชลชวีก โอลส์ไดน์ จึงอยู่ในเกณฑ์ที่ดี

ไวแซร์ตเห็นว่าการณที่หน่วยงานของรัฐที่มีการล่วงละเมิดการคุ้มครองข้อมูลส่วนบุคคลของประชาชนนั้น ส่วนใหญ่เป็นปัญหาการขาดความรู้และขาดจิตสำนึกในเรื่องสิทธิส่วนตัว อันที่จริงแล้วเจ้าหน้าที่ยอมรับหลักการเรื่องสิทธิความเป็นส่วนตัว (Privacy) แต่ยังคงชินกับประเพณีการบริหารแบบเดิม ซึ่งหากได้เรียนรู้และเข้าใจหลักการแล้วก็จะเห็นว่า หลักสิทธิความเป็นส่วนตัว

ทำให้การปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพมากขึ้น ในส่วนของประชาชนนั้น ไวเวิร์ตเห็นว่ามี ความตื่นตัวและรับรู้เรื่องสิทธิความเป็นส่วนตัวมากขึ้น และความสามารถในการจัดการที่เกี่ยวกับ ข้อมูลได้มากยิ่งขึ้น

ต่อข้อกล่าวหาที่ว่าเจ้าหน้าที่ของรัฐมักเป็นผู้ที่ล่วงละเมิดสิทธิความเป็นส่วนตัว และ ข้อมูลส่วนบุคคลมากที่สุด ดิกส์ยอมรับว่าสภาพดังกล่าวมีอยู่จริง แต่ขณะเดียวกันการล่วงละเมิด ข้อมูลส่วนบุคคลโดยภาคเอกชนก็มีมากเช่นกัน เมื่อกฎหมายคุ้มครองข้อมูลเริ่มใช้ เจ้าหน้าที่รัฐ จำนวนมากจะบอกว่าไม่สามารถปฏิบัติงานได้อีกต่อไป และอาจต้องยกเลิกวิธีการปฏิบัติงาน แบบเดิม เพราะหน่วยงานจะถูกควบคุมโดยประชาชนซึ่งจะเข้ามาควบคุมเอกสารของเขาด้วย ตนเอง จริงอยู่ที่สิทธิเข้าถึงข้อมูลข่าวสาร มีเป้าหมายในการจำกัดอำนาจของโครงสร้างการบริหาร ของภาครัฐ แต่ในอนาคตจะครอบคลุมถึงข้อมูลในภาคเอกชนด้วย

เมื่อถามถึงการให้ความสำคัญต่อเรื่องสิทธิเข้าถึงข้อมูลข่าวสาร หรือเรื่องการคุ้มครอง ข้อมูลดิกส์บอกว่า เขาให้น้ำหนักในเรื่องสิทธิเข้าถึงข้อมูลข่าวสารมากกว่า เพราะกฎหมายเพิ่ง นำมาใช้เพียง 6 ปี ขณะที่การคุ้มครองข้อมูลใช้มากกว่า 30 ปีแล้วจนนับว่าสามารถอยู่ในจิตสำนึก สาธารณะเป็นอย่างดีมากกว่า

ต่อข้อสังเกตเกี่ยวกับการละเมิดข้อมูลส่วนบุคคล ดิกส์เห็นว่าไม่ไปจะเป็นเพราะเจตนา ในการล่วงล้ำหรือละเมิด แต่บางครั้งเป็นเพราะการละเลย หรือความไม่เข้าใจของประชาชน เกี่ยวกับประเภทหรือความสำคัญของข้อมูล องค์กรที่จัดเก็บหรือระบบการประมวลข้อมูลอัตโนมัติ ในทางปฏิบัติ การคุ้มครองข้อมูลจึงไม่เน้นมาตรการการลงโทษ เพราะปัญหาอาจเกิดจากความไม่ เข้าใจอย่างแท้จริง เกี่ยวกับการจัดเก็บโดยเฉพาะโดยคอมพิวเตอร์ อาจมีข้อผิดพลาดในระบบ ประมวลผล ในซอฟต์แวร์ โปรแกรม รวมทั้งความผิดพลาดของคน (Human mistake)

3.2 การปฏิบัติงานของสำนักงานผู้ตรวจการด้านการคุ้มครองข้อมูล

สำนักงานผู้ตรวจการด้านการคุ้มครองข้อมูลของรัฐบรานเดนบวร์ก มีเจ้าหน้าที่ 15 คน ซึ่งนับว่าเป็นสำนักงานขนาดเล็ก แต่ ดิกส์อธิบายว่าไม่เป็นอุปสรรคในการทำงานแต่อย่างใด โดย สำนักงานของเขาจะพยายามทำความเข้าใจกับหน่วยงานของรัฐว่า หน้าที่ในการคุ้มครองข้อมูล ส่วนบุคคลนั้น เป็นหน้าที่ของเจ้าหน้าที่ของหน่วยงานต่างๆ มิใช่หน้าที่ของสำนักงานผู้ตรวจการฯ และเขาพยายามทำให้สำนักงานฯ เป็นตัวเร่ง (Catalyst) ในการเผยแพร่ความรู้ความเข้าใจ และใช้ วิธีการสร้างตัวขยายผล (Multipliers) เพื่อทำหน้าที่ถ่ายทอดความคิดความรู้ต่อไป เช่น ครู หรือ อาจารย์ที่มีชื่อเสียง หรือสมาชิกรัฐสภา

สำนักงานผู้ตรวจการฯ ของ เซลซวิก โฮลสไตน์ มีเจ้าหน้าที่ 30 คน งานประมาณ 30 % เป็นการแก้ปัญหาเรื่องร้องเรียนของประชาชน ขณะเดียวกัน ก็มีภารกิจด้านการเผยแพร่ประชาสัมพันธ์เพื่อเผยแพร่ความรู้และความตระหนักแก่ประชาชน มีการจัดแสดงนิทรรศการ จัดทำเอกสารเผยแพร่ ใบปลิว การเผยแพร่ผ่านบทความหนังสือพิมพ์ และผ่านอินเทอร์เน็ต รวมทั้ง การส่งเสริมให้ประชาชนตรวจสอบและคุ้มครองสิทธิความเป็นส่วนตัวส่วนตัวด้วยตัวเอง (Self Privacy Protection) เช่นในการควบคุมความเป็นส่วนตัวในอินเทอร์เน็ต (Internet Privacy) ซึ่งมีขอบเขตกว้างขวาง และมีความสำคัญมาก และสำนักงานผู้ตรวจการฯ ยังไม่สามารถควบคุมดูแลทั่วถึง

งานของผู้ตรวจการฯ ของ เซลซวิก โฮลสไตน์ มีลักษณะค่อนข้างแตกต่างจากรัฐอื่นๆ ที่อาจให้ความสำคัญงานแก้ไขปัญหาร้องเรียนเป็นหลัก แต่สำนักงานผู้ตรวจการฯ ของเซลซวิก โฮลสไตน์ เน้นงานเสริมสร้างความรู้ความเข้าใจและให้คำแนะนำปรึกษาแก่ประชาชนมากกว่า รวมทั้งการใช้ระบบ Audit ซึ่งจะเพิ่มความสำคัญมากขึ้นในอนาคต วิธีการเผยแพร่ที่สำคัญอีกประการคือ การจัดทำรายงานแถลงต่อรัฐสภาและต่อสื่อมวลชน สำนักงานผู้ตรวจการฯ ของ เซลซวิก โฮลสไตน์ จะมีการแถลงข่าวแก่สื่อมวลชนเป็นประจำทุก 2-3 เดือน โดยพยายามดึงดูดให้สื่อมวลชนสนใจซักถาม และเขียนบทความเผยแพร่ต่อไป ซึ่งเป็นวิธีการที่ได้ผล

ส่วนการเผยแพร่ความรู้ของเบอร์ลินนั้น การศึกษาใช้วิธีการเผยแพร่ผ่านสื่อมวลชน โดยเฉพาะหนังสือพิมพ์และโทรทัศน์ รวมทั้งการที่เขาและเจ้าหน้าที่ผู้เชี่ยวชาญจะออกไปบรรยายแก่สถานศึกษาต่างๆ สำนักงานของเขามีความสัมพันธ์ที่ดีกับสื่อมวลชนทั้งวิทยุ โทรทัศน์ และหนังสือพิมพ์ และกลไกเผยแพร่ที่ดีที่สุด คือ การจัดพิมพ์รายงานประจำปีเสนอต่อรัฐสภา

ไวแซร์ตียืนยันความเป็นอิสระของผู้ตรวจการฯ ว่าไม่มีผลกระทบโดยการควบคุมงบประมาณแต่อย่างใด เพราะงบประมาณได้รับการอนุมัติโดยรัฐสภา ดังนั้น ผู้ตรวจการฯ จึงสามารถปฏิบัติหน้าที่ในการควบคุมกำกับดูแลหน่วยงานของรัฐ รวมทั้งกระทรวงการคลัง โดยไม่ต้องระมัดระวังว่าถูกแทรกแซง ในส่วนของรัฐเองก็ไม่เคยมีบทบาทในการแทรกแซงการทำงานของ ผู้ตรวจการฯ เช่นกัน

สำหรับประเด็นความเป็นอิสระของผู้ตรวจการฯ ดิกส์บอกว่าแนวคิดความเป็นอิสระ และระบบผู้ตรวจราชการแผ่นดิน (Ombudsman) หรือสุนัขเฝ้าบ้าน (Watch Dog) เป็นที่ยอมรับโดยพื้นฐาน บางครั้งเขาได้วิจารณ์รัฐมนตรี และได้กลายเป็นประเด็นการถกเถียงทางการเมือง (Political Debate) หลายครั้งที่เขามีข้อคิดเห็นไม่ตรงกับหน่วยงานของรัฐ ก็จะจัดทำแถลงการณ์ต่อสาธารณะ (Public Statement) สื่อมวลชนจะมาติดตามสอบถามและวิพากษ์วิจารณ์ แต่ไม่มีผู้ใดสามารถกดดันไม่ว่าทางใดทางหนึ่ง ขณะเดียวกัน สำนักงานผู้ตรวจการฯ ไม่มีอำนาจสั่งการหน่วยงานของรัฐให้ถือปฏิบัติ แต่ทำได้เพียงจัดทำแถลงการณ์ต่อสาธารณะ หรือรายงานต่อรัฐสภา

หากเห็นว่าหน่วยงานปฏิบัติไม่ถูกต้องตามกฎหมายหรือละเมิดสิทธิส่วนตัว และหน่วยงานจะต้องไปแถลงหรือชี้แจงเหตุผลต่อสภาหรือต่อสาธารณะโดยผ่านสื่อมวลชน บทบาทของสำนักงานผู้ตรวจการฯ โดยรวม จึงไม่ใช่การเผชิญหน้ากับหน่วยงานของรัฐ (confrontation) แต่เป็นการเฝ้าระวังเสมือน Watch Dog และไม่มีผลกระทบต่อความเป็นอิสระของผู้ตรวจการฯ

บทบาทของ Watch Dog ยังปรากฏในกระบวนการแก้ไขปัญหแก่ประชาชน เพราะสำนักงานผู้ตรวจการฯ จะแก้ปัญหาเมื่อประชาชนส่งเรื่องร้องเรียนเข้ามา ซึ่งเป็นช่องทางในการเยียวยาเพิ่มขึ้นจากการใช้สิทธิฟ้องร้องทางศาล ซึ่งต้องใช้เวลาาน เพราะศาลมีคดีค้างการพิจารณาเป็นจำนวนมาก รวมทั้งมีค่าใช้จ่ายสูง ในขณะที่การร้องเรียนต่อผู้ตรวจการฯ ไม่ต้องเสียค่าใช้จ่าย และแก้ปัญหาได้รวดเร็วกว่า ผู้ตรวจการฯ จึงมีสถานะเป็น Watch Dog แก่ประชาชน ในโครงสร้างการบริหารราชการ ส่วนกรณีที่ว่าผู้ตรวจการฯ อาจทำหน้าที่ไม่สมบูรณ์ในการตรวจตราหรือเฝ้าระวังรัฐบาล เพราะรัฐเป็นผู้มอบงบประมาณให้สำนักงานผู้ตรวจการฯ ใช้ในการปฏิบัติงานนั้น ดิکشปริเยศวรว่า กระบวนการตัดสินใจเรื่องงบประมาณเป็นของรัฐสภา และผู้ตรวจการฯ มาจากการเลือกตั้งโดยรัฐสภา และได้ประกันความเป็นอิสระในการปฏิบัติงาน ผู้ตรวจการฯ จึงไม่มีการเลือกปฏิบัติเป็นพิเศษต่อกระทรวงการคลัง เพราะมีความคาดหวังเกี่ยวกับเรื่องงบประมาณแต่อย่างใด และไม่เคยมีแรงกดดันในเรื่องนี้

3.3 ความสำคัญในเรื่องการคุ้มครองข้อมูล

บัวร์เคิร์ตเห็นว่าเมื่อเปรียบเทียบการคุ้มครองข้อมูลส่วนบุคคลกับเรื่องอื่นๆ เช่น ความโปร่งใส การคุ้มครองผู้บริโภค หรือเสรีภาพของสื่อมวลชน การคุ้มครองข้อมูลส่วนบุคคลถือว่าอยู่ในเกณฑ์ที่ยอมรับกันว่าสูง แต่ไม่สูงกว่าเรื่องความโปร่งใส หรือหลักโปร่งใสอาจสำคัญกว่าเมื่อสังคมหรือรัฐมีแนวโน้มที่จะอ้างเหตุผลในเรื่อง "ความลับ" หรือ "การข่าว" ซึ่งหากไม่ยึดหลักโปร่งใส ก็อาจมีความพยายามที่จะใช้หลักการคุ้มครองข้อมูลในทางที่ผิด (Misuse of Data Protection) โดยใช้เป็นข้ออ้างในการเก็บบางเรื่องไว้เป็นความลับซึ่งขัดต่อหลักโปร่งใส

อย่างไรก็ตาม การคุ้มครองข้อมูลส่วนบุคคลก็ยังได้รับความสำคัญสูงมาก เพราะเป็นสิทธิที่ปกป้องสิทธิอย่างอื่น เช่น สิทธิในการแสดงความคิดเห็น และสิทธิในการชุมนุมโดยเสรี เช่น ในกรณีที่มีการชุมนุมหรือเดินขบวน การจดทะเบียนรถที่จอดในบริเวณที่ชุมนุมของเจ้าหน้าที่ตำรวจจะส่งผลกระทบต่อเสรีภาพในการชุมนุม เพราะประชาชนผู้มาชุมนุมย่อมไม่ต้องการให้เจ้าหน้าที่รู้หรือจดบันทึกทะเบียนรถไป ซึ่งเป็นกรณีที่เทคนิคของการสำรวจตรวจตรา (Surveillance) กำลังลดทอนเสรีภาพของบุคคล การคุ้มครองข้อมูลส่วนบุคคลจึงมีความสำคัญใน

การถ่วงดุลกับการสอดแนมหรือการตรวจตรา ในขณะเดียวกันก็เป็นการประกันและคุ้มครองสิทธิ การแสดงความคิดเห็นและสิทธิในเรื่องอื่นๆ

ต่อประเด็นคำถามว่า เจ้าหน้าที่ของรัฐมีความเข้าใจและตระหนักถึงความสำคัญของ การคุ้มครองข้อมูลหรือไม่ เช่นในกรณีที่มีการดำเนินการไม่ถูกต้องตามหลักการหรือกฎหมาย คุ้มครองข้อมูล บัรริเคอร์อธิบายว่า ในห้วงเวลาหลังๆ นี้ คือใน 5 - 10 ปีที่ผ่านมา เป็นกรณีความ ผิดพลาดของการใช้ดุลยพินิจหรือความผิดพลาดในการสร้างดุลยภาพ มากกว่าจะเป็นกรณีที่มี ความสนใจจะละเมิดสิทธิส่วนตัวหรือไม่ตระหนักเพียงพอ เพราะหน่วยงานของรัฐมีความรู้และ เข้าใจและตระหนักถึงความสำคัญของการคุ้มครองข้อมูลส่วนบุคคลเป็นอย่างดี แต่อาจให้น้ำหนัก ในการถ่วงดุลกับผลประโยชน์สาธารณะ หรือผลประโยชน์ของหน่วยงานแตกต่างกันไปตามแต่ กรณีย เช่นในกรณีหลังเหตุการณ์ 11 กันยายน ซึ่งมีประเด็นถกเถียงกันเกี่ยวกับกฎหมายต่อต้าน การก่อการร้าย (Antiterrorism Law) ว่ามหาวิทยาลัยจะสามารถประมวลข้อมูลของนักศึกษา เพื่อที่จะค้นหาบุคคลที่อยู่ในเกณฑ์ที่กำหนดได้โดยถูกกฎหมายหรือไม่ ซึ่งเป็นประเด็นที่ต้อง ถกเถียงกันถึงดุลยภาพระหว่างผลประโยชน์สาธารณะ ซึ่งหมายถึงความมั่นคงปลอดภัยของชาติ และสิทธิความเป็นอยู่ส่วนตัวของนักศึกษา ซึ่งจะต้องหาจุดดุลยภาพที่เหมาะสมที่สุดและประเด็น สำคัญคือต้องไม่ละเมิดสิทธิส่วนตัวอย่างร้ายแรง

4. นโยบายด้านการคุ้มครองข้อมูลของรัฐบาลในลักษณะที่เป็นนโยบายแห่งรัฐและความเชื่อมโยง กับพรรคการเมืองและสื่อมวลชน

บัรริเคอร์อธิบายว่าไม่มีความเชื่อมโยงทางการเมืองโดยตรงระหว่างผู้ตรวจการฯ กับ พรรคการเมือง เพราะผู้ตรวจการฯ จะปฏิบัติหน้าที่อย่างเป็นกลาง (Neutrality) เพราะได้รับการ แต่งตั้งโดยรัฐสภา ซึ่งมีแนวโน้มที่จะเป็นกระบวนการแต่งตั้งที่ปลอดการเมือง (Non Political Party Issue) มากกว่าจะเลือกบุคคลที่สังกัดพรรคการเมือง และเมื่อได้รับการแต่งตั้งแล้ว ผู้ตรวจการฯ จะมีอำนาจในการดำเนินงานเช่นเดียวกับผู้พิพากษา คือมีความเป็นกลางไม่ว่าพรรคการเมืองใด จะครองอำนาจรัฐ และผู้ตรวจการฯ ย่อมสามารถให้คำแนะนำแก่รัฐบาลเกี่ยวกับมาตรการการ คุ้มครองข้อมูลส่วนบุคคล ที่รัฐบาลควรต้องปฏิบัติ

ต่อประเด็นความเชื่อมโยงของนโยบายในเรื่องการคุ้มครองข้อมูลส่วนบุคคลกับ นโยบายแห่งรัฐในระดับชาติหรือพรรคการเมือง ไบรเอร์อธิบายว่า การปฏิบัติในเรื่องนี้มีความ แตกต่างกันไปแต่ละรัฐ เช่นกรณีรัฐบรานเดนบวร์ก ซึ่งมีบทบัญญัติว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล และเรื่องสิทธิเข้าถึงข้อมูลข่าวสารปรากฏอยู่ในรัฐธรรมนูญ ในขณะที่เชลสวิค โฮลสไตน์ไม่

มีบทบาทญัตติลักษณะดังกล่าว แต่เรื่องนี้ไม่มีผลต่อการปฏิบัติงานตามปกติแต่อย่างใด อย่างไรก็ตาม ไวแชร์ตให้ข้อสังเกตที่น่าสนใจในประเด็นความเชื่อมโยงกับนโยบายพรรคการเมือง เช่นกรีน พรรคกรีน (Green Party) ซึ่งให้ความสำคัญของประเด็นการคุ้มครองเสรีภาพส่วนบุคคลมาก ในขณะที่พรรคอนุรักษนิยมจะให้ความสำคัญแก่ประเด็นความมั่นคง (Security) มากกว่า แต่ในขณะเดียวกันนโยบายก็จะผันแปรตามสถานการณ์ทางการเมือง เช่นเมื่อพรรคกรีนเข้าร่วมรัฐบาล กลับยอมรับให้ออกกฎหมายต่อต้านการก่อการร้าย (Antiterrorism Law) ซึ่งมีเนื้อหาหลายประการขัดกับหลักการคุ้มครองสิทธิความเป็นส่วนตัว

ไวแชร์ตเห็นว่าการมีบทบาทญัตติเรื่องสิทธิในความเป็นส่วนตัว (Privacy) ในรัฐธรรมนูญ ก็มีความสำคัญ เช่นกรีนประเทศไทยหรืออเมริกา โดยเฉพาะในอเมริกาซึ่งการยอมรับหลักการเรื่องสิทธิในความเป็นส่วนตัวมีสูงมาก การเขียนเรื่องสิทธิในความเป็นส่วนตัว ในรัฐธรรมนูญ ก็จะเป็นประโยชน์ เช่นหากจะหยิบยกขึ้นมาเป็นประเด็นคัดค้านกฎหมายต่อต้านการก่อการร้ายของรัฐบาล บุษ เพราะกฎหมายดังกล่าวมีผลน้อยมากต่อผู้ก่อการร้าย แต่ผลกระทบอย่างร้ายแรงต่อการควบคุมและการแทรกแซงชีวิตส่วนตัวของประชาชน

สำหรับด้านสื่อมวลชนนั้น บัวร์เคิร์ตอธิบายว่า สื่อมวลชนจะให้ความสนใจในเรื่องที่เป็นเรื่องอื้อฉาว (Scandal) และเรื่องเกี่ยวกับเรื่องส่วนตัวของบุคคล จึงมักเกิดความขัดแย้งกับหน่วยงานของรัฐเมื่อสื่อต้องการให้เปิดเผยในเรื่องที่เป็นข้อมูลส่วนตัวบุคคล ในขณะที่หน่วยงานเห็นว่าเป็นข้อมูลที่ต้องคุ้มครอง ดังนั้น กรณีสวนใหญ่จึงเป็นเรื่องของการคุ้มครองข้อมูลที่ยังไม่เพียงพอและการคุ้มครองที่มากเกินไป ในขณะเดียวกันสื่อมวลชนก็มีแนวโน้มที่จะเป็นผู้ล่งละเมิดสิทธิความเป็นอยู่ส่วนตัวเช่นกัน ไม่ว่าจะเป็นกรณีการเปิดเผยข้อมูลส่วนตัว หรือกิจกรรมส่วนตัวของนักการเมือง และโดยเฉพาะกรณีการเผยแพร่ภาพหรือข้อมูลเกี่ยวกับเหยื่อหรือญาติของเหยื่อในคดีอาชญากรรม และในกรณีที่ข้อมูลที่เป็นเรื่องเฉพาะตัว (Sensitive Data) ของประชาชน ซึ่งเป็นประเด็นเกี่ยวกับดุลยภาพระหว่างการคุ้มครองสิทธิความเป็นอยู่ส่วนตัวของประชาชน ไม่ว่าจะเป็นนักการเมืองหรือประชาชนทั่วไป

ในทางปฏิบัติจะมีองค์กรควบคุมทางวิชาชีพ (Self Regulating Body) ของสื่อมวลชน ซึ่งองค์กรดังกล่าวจะมีประกาศหรือแจ้งตักเตือนไปยังสื่อมวลชนที่ไม่ระมัดระวังในการเสนอข้อมูลที่ไม่เหมาะสม แต่กลไกดังกล่าวยังไม่มีประสิทธิภาพเท่าที่ควรเพราะสื่อมวลชนจะดำเนินการบนพื้นฐานผลประโยชน์ทางธุรกิจในการขายข่าว มากกว่าการรักษาผลประโยชน์หรือชื่อเสียงของเหยื่อซึ่งเป็นประชาชน ซึ่งประชาชนต้องไปใช้สิทธิทางศาลในการเรียกร้องค่าเสียหายชดเชย ซึ่งจะเป็นกรณีการเยียวยาหลังจากได้มีการล่งละเมิดไปแล้ว อย่างไรก็ตาม การฟ้องคดีต่อศาลมีค่าใช้จ่ายที่คนจนไม่สามารถแบกรับได้ ขณะเดียวกัน ประชาชนบางส่วนก็ยังไม่ให้ความสำคัญใน

เรื่องดังกล่าวมากนัก รวมทั้งยังมีอีกบางส่วนที่นำเรื่องส่วนตัวของเพื่อนบ้านไปขายแก่สื่อมวลชน อันเป็นการร่วมกันกับสื่อมวลชนลวงละเมิดข้อมูลส่วนบุคคล อย่างไรก็ตามความตระหนักถึงอันตรายจากการละเมิดข้อมูลส่วนบุคคลโดยสื่อมีเพิ่มมากขึ้นในปัจจุบัน

5. ระบบการตรวจสอบการคุ้มครองโดยผู้ตรวจสอบ (Auditor) ของเชลสวิค โฮลสไตน์ (Schleswig Holstein)

ไวแซร์ตอธิบายถึงระยะการควบคุมและการตรวจสอบการคุ้มครองข้อมูลส่วนบุคคลของเชลสวิค โฮลสไตน์ โดยการใช้ระบบที่ดำเนินการโดยผู้ตรวจสอบ (Auditor) และการออกสัญลักษณ์รับรองในลักษณะใบรับรอง (Certificate) หรือใบอนุญาต (License)

ไวแซร์ตอธิบายว่าแนวความคิดนี้เกิดขึ้นเนื่องจากภาคเอกชนจำนวนมากซึ่งอยู่ภายใต้กฎหมายคุ้มครองข้อมูลส่วนบุคคลประสงค์ปฏิบัติตามกฎหมาย แต่ไม่รู้ว่าจะปฏิบัติได้อย่างไร สำนักงานผู้ตรวจการฯ ของเขาจึงเสนอให้มีผู้เชี่ยวชาญเข้าไปตรวจสอบระบบการคุ้มครองข้อมูลส่วนบุคคล ให้แก่หน่วยงานหรือองค์กรต่างๆ ที่แสดงความจำนง โดยเมื่อผู้เชี่ยวชาญเข้าไปศึกษาระบบ และจัดวางระบบการคุ้มครองข้อมูลส่วนบุคคลที่ถูกต้อง หรือพัฒนาหรือปรับปรุงแก้ไขให้อยู่ในเกณฑ์มาตรฐานแล้ว ก็จะออกหลักฐานเป็นใบรับรอง หรือสัญลักษณ์รับรองการคุ้มครองสิทธิความเป็นส่วนตัว (Privacy Mark) วิธีการนี้ได้รับความนิยมมาก และได้พัฒนาไปสู่การตรวจสอบรับรองผลิตภัณฑ์ หรือสินค้าที่เกี่ยวข้องกับข้อมูล (Information Product) เช่นในธุรกิจคอมพิวเตอร์ ซอฟต์แวร์ หรือโทรคมนาคม อุปกรณ์ติดต่อสื่อสาร เช่น โทรศัพท์ และอินเทอร์เน็ต ที่ต้องมีการคุ้มครองข้อมูลส่วนบุคคล เช่นกรณีการรับรองให้กับบริษัทที่ผลิตอุปกรณ์หรือระบบข้อมูลทางการแพทย์ เพราะแพทย์อาจเกรงว่าหากสินค้าหรือระบบไม่มีการคุ้มครองข้อมูลส่วนตัวที่ดี ความลับของคนไข้ก็จะได้รับผลกระทบ และเขาจะรู้สึกเชื่อมั่นมากยิ่งขึ้นที่จะซื้อสินค้าที่ได้รับการตรวจสอบและรับรองโดยผู้ตรวจสอบ (Auditor) และโดยหน่วยงานที่รับรองการคุ้มครองสิทธิส่วนตัว (Privacy Protection Agency) นอกจากนี้ ผู้ผลิตยังสามารถใช้ประโยชน์จากใบรับรองการตรวจสอบในการขาย การโฆษณาและประชาสัมพันธ์ ระบบตรวจสอบโดยผู้ตรวจสอบนี้ ทำให้ลักษณะการทำงานของสำนักงานผู้ตรวจการฯ มีลักษณะเป็นการวางระบบและควบคุมกระบวนการ (Procedure Supervising) และเป็นองค์กรในการกำกับและให้คำปรึกษาแก่ประชาชน (Consulting)

ถึงแม้จะเพิ่งเริ่มใช้ระบบนี้ได้ไม่นานนัก แต่ก็ได้รับความนิยมมาก ทั้งในภาคเอกชนและประชาชน เพราะโดยที่การคุ้มครองข้อมูลส่วนบุคคล เป็นเรื่องของการบังคับใช้กฎหมาย การ

ควบคุมการปฏิบัติตามระเบียบ หรือการอนุญาตให้ปฏิบัติตามกฎหมาย แต่ระบบนี้เป็นครั้งแรกของการใช้เครื่องมือทางเศรษฐกิจ (Economic Instrument) โดยการใช้ระบบตรวจสอบ (Audit) เป็นเครื่องมือในการสร้างความตระหนักและส่งเสริมสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล อย่างไรก็ตาม จะยังคงต้องมีการพัฒนาในเรื่องนี้ต่อไป โดยจะต้องมีการปรึกษาระหว่าง นักกฎหมาย นักเศรษฐศาสตร์ ผู้เชี่ยวชาญเทคโนโลยีสารสนเทศ และภาคธุรกิจเทคโนโลยีสารสนเทศ ไวแอิร์ตเน้นว่า ระบบการกำกับโดยใช้เครื่องมือทางเศรษฐกิจของระบบตรวจสอบนี้ จะเป็นทิศทางในอนาคตของการคุ้มครองข้อมูล

สำนักงานผู้ตรวจการฯ ของเชลสวิค โฮลสไตน์ ยังคงมีปัญหการปฏิบัติงานด้วยความไม่เพียงพอของทรัพยากร ทั้งบุคคลและงบประมาณ โดยเฉพาะไม่สามารถควบคุมดูแลภาคเอกชน นับพันหน่วยงานที่มีการเก็บและประมวลผลข้อมูลส่วนบุคคลได้ทั่วถึง Schleswig-Holstein จึงใช้ระบบให้ผู้เชี่ยวชาญออกไปทำการตรวจสอบ (Audit) แทนการออกไปตรวจสอบด้วยตนเอง

ลักษณะเด่นของ สำนักงานผู้ตรวจการฯ ของเชลสวิค โฮลสไตน์อีกประการหนึ่ง คือการจัดตั้งสถาบันด้านการคุ้มครองข้อมูล (Data Protection Academy) เพื่อดำเนินการจัดหลักสูตรฝึกอบรมความรู้เรื่องการคุ้มครองข้อมูลแก่เจ้าหน้าที่ของสำนักงานผู้ตรวจการฯ ต่างๆ รวมทั้งเจ้าหน้าที่ขององค์กรภาคเอกชน ซึ่งมีหลักสูตรหลากหลายทั้งด้านกฎหมาย ด้านเทคนิคการปฏิบัติตามกฎหมาย การควบคุมการปฏิบัติตามกฎหมาย ด้านเทคโนโลยีสารสนเทศ ฯลฯ ซึ่งได้รับความสนใจจากหน่วยงานต่างมาเข้าร่วมศึกษาอบรมเป็นจำนวนมากในแต่ละปี

6. ปัญหาการกำกับดูแลการคุ้มครองข้อมูลในภาคเอกชน

ปัญหาในการปฏิบัติงานอีกประการหนึ่ง ก็คือปัญหาการกำกับดูแลการคุ้มครองข้อมูลในภาคเอกชน เพราะสำนักงานผู้ตรวจการฯ จะควบคุมการปฏิบัติตามกฎหมายของหน่วยงานรัฐบาลเท่านั้น ในขณะที่การกำกับดูแลการเก็บข้อมูลส่วนบุคคลของภาคเอกชนจะเป็นหน้าที่ของหน่วยงานในสังกัดกระทรวงมหาดไทย ซึ่งมีวัฒนธรรมในองค์กรเฉพาะ เนื่องจากเป็นหน่วยปฏิบัติงานที่เกี่ยวข้องกับตำรวจหรือหน่วยงานราชการลับ ทำให้การปฏิบัติงานในส่วนนี้ขาดความเป็นอิสระอย่างแท้จริง ในส่วนของผู้ตรวจการฯ นั้น ไม่มีปัญหาความเป็นอิสระ เพราะได้รับการเลือกตั้งโดยรัฐสภา แต่ไวแอิร์ตก็ยังเห็นว่ารูปแบบองค์กรที่ดีที่สุดสำหรับการคุ้มครองข้อมูลส่วนบุคคล คือการควบคุมที่หน่วยงานของรัฐและหน่วยงานภาคเอกชน อยู่ภายใต้สำนักงานผู้ตรวจการฯ เดียวกัน

นอกจากนี้ การ์สคาบอกล่าวเนื่องจากผู้บริหารระดับสูงของกระทรวงมหาดไทยส่วนใหญ่จะไม่ให้ความสำคัญกับงานการคุ้มครองข้อมูล ความตื่นตัวเรื่องสิทธิในความเป็นส่วนตัวในภาคเอกชนในช่วงแรกจึงค่อนข้างน้อย

การ์สคาอธิบายว่าปัญหาการคุ้มครองข้อมูลของเยอรมัน ได้พัฒนามาตลอด 30 ปี ปัญหาปัจจุบันจะอยู่ในเรื่องของภาคเอกชน การตลาด และความมั่นคง โดยเฉพาะหลังเหตุการณ์ 11 กันยายน มาตรการในกฎหมายต่อต้านการก่อการร้ายส่งผลกระทบต่อเรื่องการคุ้มครองข้อมูลส่วนบุคคลโดยตรง นอกจากนี้จะยังส่งผลกระทบต่อธุรกิจโทรคมนาคมและสื่อสาร เช่น บริษัทโทรศัพท์ และผู้ให้บริการอินเทอร์เน็ต เพราะพวกเขาต้องคิดถึงผลกระทบต่อประชาชน ซึ่งเป็นลูกค้าในบริการของเขา

ดิกส์ อธิบายว่าปัญหาสำคัญในเรื่องการคุ้มครองข้อมูลและสิทธิความเป็นส่วนตัวของเยอรมัน(Privacy Champion) คือประเด็นกฎหมายต่อต้านอาชญากรรมและการก่อการร้าย ประเทศตะวันตกหลายประเทศมีการออกกฎหมายดังกล่าว โดยมีพื้นฐานความเชื่อว่าการเก็บข้อมูลส่วนบุคคลจะสามารถแก้ปัญหานี้ได้ โดยเฉพาะการเก็บข้อมูลโดยกล้องเฝ้ามอง (VDO Surveillance) การตรวจผู้ผ่านแดนโดยการบรรจุข้อมูลทางชีวภาพ (Biometric Information) ในหนังสือเดินทางหรือบัตรประจำตัว ความเชื่อที่ว่า การเก็บข้อมูลไว้อย่างมากมายจะแก้ปัญหการก่อการร้ายได้ ทำให้ประชาชนจำนวนมากกังวลว่าข้อมูลจะถูกจัดเก็บในฐานข้อมูลหน่วยงานด้านความมั่นคง สำนักงานผู้ตรวจการฯ ให้ความสนใจในเรื่องนี้ เนื่องจากเป็นการให้อำนาจให้หน่วยงานความมั่นคงมากขึ้น ในขณะที่มีการเก็บข้อมูลส่วนบุคคลมากกว่าที่เคยมีการเก็บในอดีต จึงต้องมีการตรวจสอบว่า การปฏิบัติดังกล่าวเป็นไปตามหลักการคุ้มครองอย่างถูกต้องหรือไม่ นอกจากนี้ ยังมีประเด็นการเก็บข้อมูลพันธุกรรมในทางการแพทย์ ซึ่งเป็นเรื่องที่สลับซับซ้อนมาก รวมทั้งประเด็นปัญหาที่เทคโนโลยีมีการพัฒนารวดเร็วมาก จนกระบวนการบัญญัติกฎหมายพัฒนาไม่ทันเทคโนโลยีที่ภาคเอกชนหรือประชาชนนำมาใช้

นอกจากนี้ ยังรวมถึงปัญหาข้อบังคับของสหภาพยุโรป (EU Directives) เรื่องการสำรวจตรวจตราในข้อมูลข่าวสารที่ Online หรือในเครือข่ายการสื่อสาร (Communication Network) ดิกส์มีข้อสงสัยว่าหน่วยงานด้านความมั่นคงจะสามารถเก็บข้อมูลมหาศาลได้ทันเวลาหรือไม่ และทางออกที่ดีน่าจะอยู่ที่การเก็บและวิเคราะห์ข้อมูลเมื่อมีเหตุการณ์ร้ายเกิดขึ้น การที่หน่วยงานอ้างเหตุผลด้านความมั่นคงและปลอดภัย ส่งผลกระทบต่อความเป็นส่วนตัว บรรยาภาคของการสำรวจตรวจตราโดยทั่วไป (General Surveillance) เป็นประเด็นที่มีความสัมพันธ์เชื่อมโยงระหว่างประเด็นความมั่นคง (Security) และเสรีภาพ (Liberty) ข้อบังคับของสหภาพยุโรปยอมให้มีการเก็บข้อมูลให้มากที่สุด โดยไม่คำนึงถึงต้นทุนที่เกิดขึ้นทั้งต้นทุนในการทำลายสิทธิในความ

เป็นส่วนตัวและต้นทุนการจัดเก็บข้อมูลซึ่งต้องจัดเก็บจำนวนมหาศาล ดิกส์เห็นว่าไม่น่ามีข้อขัดข้อง หากจะดำเนินการจัดเก็บข้อมูลที่จำเป็นเมื่อมีข้อสงสัยเมื่อมีสถานการณ์หนึ่งเกิดขึ้น แต่กรณีที่เกิดขึ้นในปัจจุบัน เป็นกรณีที่ทำการเก็บข้อมูลเชิงป้องกัน (Preventive Routine Storage) ของข้อมูลสื่อสาร (Connecting Data) ทุกประเภท โดยปราศจากข้อสงสัยหรือสถานการณ์ใดๆ ทั้งสิ้น ซึ่งเป็นวิธีการที่ผิดมาตั้งแต่ต้น แม้สหภาพยุโรปจะประกาศใช้ข้อบังคับดังกล่าว แต่ดิกส์ยังเห็นว่ามีความเป็นไปได้ที่เยอรมันอาจไม่นำบทบัญญัติดังกล่าวมาใช้ ทั้งนี้ได้หมายความว่าเยอรมันในฐานะสมาชิกของสหภาพยุโรปจะไม่ปฏิบัติตามข้อบังคับดังกล่าว แต่รัฐธรรมนูญเยอรมันก็มีบทบัญญัติที่ไม่อนุญาตให้มีการเก็บข้อมูลการสื่อสาร หากปราศจากเหตุผลเฉพาะเป็นรายกรณี

เนื่องจากข้อบังคับของสหภาพยุโรป บัญญัติให้อำนาจแก่รัฐสมาชิกที่จะออกกฎหมายให้ Internet Provider หรือ Telecommunication Provider เก็บรวบรวมข้อมูลการสื่อสารเป็นการประจำ (Routine) ซึ่งรัฐบาลบางประเทศอาจออกกฎหมายดังกล่าว แต่รัฐบาลแห่งอาจไม่ดำเนินการ ดิกส์ไม่เห็นด้วยกับการออกกฎหมายเพื่อการเก็บข้อมูลในลักษณะที่เป็นการประจำ โดยเห็นว่าเรื่องนี้อาจต้องเข้าสู่การพิจารณาของศาลรัฐธรรมนูญ เนื่องจากอาจเป็นกรณีความสัมพันธ์ระหว่างบทบัญญัติของสหภาพยุโรป กับกฎหมายรัฐธรรมนูญของเยอรมัน

อย่างไรก็ตามเรื่องนี้ยังไม่เป็นที่ตระหนักสำหรับประชาชนทั่วไปนัก ความสนใจส่วนใหญ่จะอยู่ในวงการสื่อสารมวลชนและบริษัทเอกชนซึ่งได้รับผลกระทบโดยตรง รวมทั้งองค์กรในวงการอินเทอร์เน็ต เช่น Electronic Frontier Foundation ซึ่งมีการเสนอประเด็นในเรื่องดังกล่าว แต่การเคลื่อนไหวในภาคประชาสังคม (Civil Rights) ไม่ตื่นตัวนักเมื่อเทียบกับในอเมริกา ซึ่งดิกส์เห็นว่า ในสภาพการณ์ที่ภาคประชาชนทั่วไปยังตื่นตัวและตระหนักรู้น้อย จึงเป็นหน้าที่สำนักงานของเขาจะต้องทำเรื่องนี้ให้เป็นประเด็นสาธารณะ และทำให้ประชาชนตระหนักถึงผลกระทบที่จะมีต่อเสรีภาพในการแสดงออกที่อาจถูกละเลยหรือมองข้าม (Unobserved Freedom of Movement)

ส่วนประเด็นดุลยภาพระหว่างความมั่นคง (Security) และเสรีภาพ (Liberty) นั้น ดิกส์เห็นว่าเป็นปัญหาสำคัญและเป็นประเด็นที่ยากต่อการวินิจฉัย ถึงแม้จะไม่ได้หมายความว่าสิทธิความเป็นส่วนตัวเป็นสิ่งที่จำกัดไม่ได้ และเหตุผลในประเด็นประโยชน์สาธารณะ (Public Interest) และความปลอดภัยของประชาชน (Public Safety) ก็จะต้องมาก่อนเสมอ แต่ดิกส์ยืนยันความสำคัญของสิทธิในความเป็นส่วนตัว โดยเขาไม่เห็นด้วยในการใช้มาตรการทั่วไปในการตรวจตรา (General Measure of Surveillance) ว่าจะสามารถแก้ปัญหาความมั่นคงได้อย่างสมบูรณ์ จึงต้องใช้หลักความได้สัดส่วน (Proportional) ในการพิจารณาซึ่งน้ำหนักระหว่างเสรีภาพและความมั่นคง

7. ทิศทางและความท้าทายในอนาคต

ในขณะที่ประเทศสหพันธ์สาธารณรัฐเยอรมนีมีกฎหมายคุ้มครองข้อมูลมากกว่า 30 ปี แต่เพิ่งจะมีกฎหมายว่าด้วยการเข้าถึงข้อมูลข่าวสาร (Information Access Act or Freedom of Information Act) เมื่อ 3-4 ปีที่ผ่านมา ยังเป็นกฎหมายในระดับรัฐ (State Act) เท่านั้น ยังไม่มีกฎหมายในระดับชาติ (Federal Act) ซึ่งขณะนี้อยู่ระหว่างการดำเนินการจัดทำร่างกฎหมาย ปัจจุบันรัฐที่มีการประกาศใช้กฎหมายข้อมูลข่าวสารแล้วได้แก่ รัฐบรานเดนบวร์ก นอร์ทไรน์-เวสต์ฟาเลีย (Northrhine Westphalia) เซลซวิก-โฮลสไตน์ และมหานครเบอร์ลิน ปัจจุบันรัฐดังกล่าวมีรูปแบบการดำเนินการตามกฎหมายเหมือนกัน คือการดำเนินการตามกฎหมายข้อมูลข่าวสารอยู่ภายใต้การกำกับดูแลของผู้ตรวจการฯ นั่นก็คือผู้ตรวจการฯ ของ 3 รัฐ และผู้ตรวจการฯ ของเบอร์ลินเป็นผู้ใช้อำนาจตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล และกฎหมายว่าด้วยการเข้าถึงข้อมูลข่าวสารนั่นเอง

จากการสนทนาแลกเปลี่ยนความคิดเห็นและสัมภาษณ์ผู้ตรวจการฯ และเจ้าหน้าที่ผู้รับผิดชอบของสำนักงานผู้ตรวจการฯ ของทุกรัฐ มีความเห็นตรงกันว่า การบริหารบังคับใช้กฎหมายทั้ง 2 ฉบับ โดยอยู่ภายใต้ผู้ตรวจการฯ และสำนักงานของผู้ตรวจการฯ เดียวกัน เป็นวิธีที่มีประสิทธิภาพที่สุด และคาดว่ารัฐที่เหลือทั้งหมดซึ่งอยู่ระหว่างการจัดทำร่างกฎหมายมลรัฐ จะกำหนดให้มีรูปแบบเดียวกัน คือมีผู้ตรวจการฯ คนเดียวในการกำกับดูแลงานทั้งสองด้าน รวมทั้งร่างกฎหมายว่าด้วยการเข้าถึงข้อมูลข่าวสารแห่งสหพันธ์รัฐ (Federal Freedom of Information Act) ก็กำหนดให้ผู้ตรวจการด้านการคุ้มครองข้อมูลของสหพันธ์รัฐ ดูแลงานของกฎหมายว่าด้วยการเข้าถึงข้อมูลข่าวสารเช่นกัน

เมื่อถามถึงปัญหาสำคัญในปัจจุบันและอนาคตของ การคุ้มครองข้อมูลในเยอรมัน บัวร์เคิร์ตอธิบายว่าสิ่งที่อันตรายที่สุดคือการที่การปฏิบัติงานด้านการคุ้มครองข้อมูลมีการพัฒนาจนมีลักษณะเป็นงานประจำ (Routine) ทำให้เจ้าหน้าที่ปฏิบัติงานไปตามแบบแผนโดยไม่ได้ตระหนักถึงเหตุผลหรือความรู้ในเรื่องการคุ้มครองสิทธิในความเป็นส่วนตัว ซึ่งบัวร์เคิร์ตเห็นว่าเป็นอันตรายและพึงระมัดระวัง เพราะธรรมชาติของระบบราชการซึ่งมีการปฏิบัติงานในลักษณะงานประจำ (Routine) ซึ่งเน้นการปฏิบัติตามขั้นตอนโดยละเอียดหรือไม่ให้ความสำคัญกับการใช้ดุลยพินิจหรือการพิจารณาบนพื้นฐานปรัชญาของการคุ้มครองข้อมูลส่วนบุคคล บัวร์เคิร์ตย้ำว่า สำนักงานผู้ตรวจการฯ จะต้องมีความเป็นองค์กรที่มีชีวิตและจะมีบทบาทมากขึ้นในอนาคต โดยเฉพาะจะต้องพัฒนาให้รองรับการพัฒนาเทคโนโลยีในอนาคต ขณะเดียวกันต้องสามารถใช้เทคโนโลยีในการพัฒนาและเสริมสร้างมาตรการคุ้มครองข้อมูลด้วย (Privacy Enhancing Technology) ผู้ตรวจการฯ จึงต้องมีความตื่นตัวและพัฒนาตัวเอง ด้วยการใช้เทคโนโลยีสมัยใหม่

ในการพัฒนาระบบให้มีประสิทธิภาพสูง ในขณะที่จะต้องลดต้นทุนในการคุ้มครองสิทธิในความเป็นส่วนตัว (Make system effective but at less cost to privacy)

ประเด็นการเผยแพร่ความรู้เกี่ยวกับ การคุ้มครองข้อมูล ยังคงมีความสำคัญและเป็นเรื่องจำเป็น เพราะการคุ้มครองข้อมูลไม่เพียงจำเป็นต่อนักกฎหมาย แต่ยังมีความสำคัญต่อนักวิจัยโดยทั่วไป ไม่ว่าจะเป็นสาขาวิทยาศาสตร์ สังคมศาสตร์ สังคมวิทยา แพทย์ นักศึกษาแพทย์ เพราะนักวิชาการที่ทำการวิจัยจะต้องเกี่ยวข้องกับข้อมูลส่วนบุคคลของประชาชนที่เป็นประชากรในการวิจัย การเผยแพร่ความรู้เกี่ยวกับการคุ้มครองข้อมูล จึงจำเป็น ซึ่งอาจทำได้โดยกระบวนการเรียนการสอน การกำหนดหลักสูตรในมหาวิทยาลัย รวมทั้งการเผยแพร่ผ่านสื่อมวลชนต่างๆ เช่น การเขียนบทความ โปสเตอร์ เอกสารแนะนำ และอาจใช้รูปแบบและเทคนิคที่หลากหลายในการโฆษณา เช่น การ์ตูน หรือสื่อโฆษณาอื่นๆ เช่น วิทยุ โทรทัศน์ และอินเทอร์เน็ต

นอกจากนี้ การปฏิบัติงานของสำนักงานผู้ตรวจการฯ มีภารกิจสำคัญ 3 ด้าน คือ งานนโยบาย งานการควบคุมและบังคับใช้กฎหมาย และงานสืบสวนสอบสวนเรื่องร้องเรียนของประชาชน ซึ่ง บัณฑิตเห็นว่าการใช้เจ้าหน้าที่ซึ่งมีไม่เพียงพออยู่แล้ว ไปปฏิบัติงานในเรื่องการบังคับใช้กฎหมายและเรื่องร้องเรียนมากเกินไป และผู้ตรวจการฯ ควรให้ความสนใจในการปฏิบัติงานในเรื่องนโยบาย ซึ่งมีภารกิจสำคัญ 2 ประการ คือ

1. การพิจารณาเกี่ยวกับการออกหรือพัฒนาข้อกฎหมาย เมื่อหน่วยงานหรือรัฐบาลเสนอร่างกฎหมายใหม่ ผู้ตรวจการฯ จะต้องพิจารณาว่ากฎหมายดังกล่าว สอดคล้องกับหลักการในเรื่องสิทธิความเป็นอยู่ส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคลหรือไม่ และควรจะต้องให้ความเห็นต่อร่างกฎหมายดังกล่าว โดยที่ไม่มีข้อปฏิบัติหรือกฎหมายที่บัญญัติให้ร่างกฎหมายของรัฐบาลจะต้องส่งมาที่สำนักงานผู้ตรวจการฯ ก่อน และโดยที่บางครั้ง บางหน่วยงานพยายามที่จะหลบเลี่ยงความสนใจของผู้ตรวจการฯ จึงน่าจะเป็นการดีหากจะมีระเบียบปฏิบัติไว้ว่า หากรัฐบาลมีข้อเสนอร่างกฎหมายใหม่ โดยเฉพาะกฎหมายซึ่งเกี่ยวข้องหรือมีผลบังคับในกรณีจะมีการเก็บข้อมูลส่วนบุคคล ใหม่ หรือเมื่อจะมีการใช้ ข้อมูลส่วนบุคคล น่าจะต้องผ่านกระบวนการให้ความเห็นของผู้ตรวจการฯ

ทั้งนี้ บัณฑิตบอกว่า เขาไม่ได้หมายถึงการใช้อำนาจยับยั้งร่างกฎหมายโดยผู้ตรวจการด้านการคุ้มครองข้อมูล เพราะเป็นอำนาจของรัฐบาล แต่ผู้ตรวจการด้านการคุ้มครองข้อมูล ควรแสดงความเห็นในกรณีดังกล่าว ด้วยเหตุนี้ จำนวนเจ้าหน้าที่จึงไม่เพียงพอที่จะทำงานด้านนโยบาย โดยเฉพาะเจ้าหน้าที่ที่มีพื้นฐานความรู้ด้านอื่นๆ เช่น รัฐศาสตร์ ซึ่งจะมีความเข้าใจกระบวนการทางการเมืองและมีมุมมองปัญหาที่กว้างกว่าเจ้าหน้าที่ฝ่ายเทคนิคเท่านั้น

2. การพิจารณาเกี่ยวกับพัฒนาการในอนาคต ผู้ตรวจการฯ จะต้องมีความสามารถในการพิจารณากำหนดนโยบายล่วงหน้า เพราะโลกปัจจุบันมีการพัฒนาทางเทคโนโลยีรวดเร็วมาก

เช่น กรณีการใช้โทรศัพท์มือถือที่สามารถระบุกำหนดจุดที่ผู้ใช้อยู่ได้ หรือการเก็บข้อมูลการเดินทาง ขณะที่จ่ายค่าผ่านทาง หรือการฝังแผ่นความจำ (Chip) ได้มีหวังมนุษย์ เพื่อให้สามารถติดตาม ค้นหาได้ว่าบุคคลอยู่ที่ไหน หลายกรณิดังกล่าวเป็นกรณีที่เกี่ยวข้องกับหลักการคุ้มครองข้อมูลส่วนบุคคล ซึ่งผู้ตรวจการฯ จะต้องเข้าใจพัฒนาการที่รวดเร็ว และต้องตระหนักและเตรียมนโยบายที่สอดคล้องกับเทคโนโลยีดังกล่าว

บทสรุป

จากการศึกษาและเรียนรู้ประสบการณ์ของเยอรมันข้างต้น เน้นย้ำให้เห็นว่า “ข้อมูลส่วนบุคคล” มีฐานะเป็นสิทธิชนิดหนึ่งของ “สิทธิในความเป็นส่วนตัว” และมีฐานะเป็นเครื่องบังที่ “ศักดิ์ศรีความเป็นมนุษย์” รัฐจึงจะต้องให้ความคุ้มครองประชาชนในเรื่องสิทธิความเป็นส่วนตัว ในเชิงข้อมูล (Informational Privacy) อย่างเต็มที่ โดยรัฐจะต้องรับประกันว่าประชาชนเป็นผู้มีสิทธิที่จะตัดสินใจให้มีการดำเนินการใดๆ เกี่ยวกับข้อมูลส่วนบุคคลของตนเอง ไม่ว่าจะเป็นการเก็บ รวบรวม ประมวลผล และใช้ประโยชน์ รัฐและบุคคลทั่วไปต้องให้ความเคารพและไม่เข้าไปแทรกแซงในสิทธิความเป็นส่วนตัวดังกล่าว

การออกมาตรการทางกฎหมายเพื่อการคุ้มครองข้อมูลส่วนบุคคลจึงเป็นเรื่องสำคัญ และจำเป็นในระดับนโยบายแห่งรัฐ (National Agenda) โดยเฉพาะมาตรการทางกฎหมายเป็นข้อเสนอสำคัญเพื่อการคุ้มครองป้องกันการรุกรานชีวิตส่วนตัว การละเมิดในสิทธิประโยชน์ส่วนตัว และการทำให้เสื่อมเสียชื่อเสียงหรือความเป็นอยู่ในชีวิตส่วนตัว อันเป็นการละเมิดศักดิ์ศรีความเป็นมนุษย์ จึงมีความจำเป็นอย่างมากที่ต้องมีกฎหมายเพื่อคุ้มครองและควบคุมการใช้ประโยชน์ในข้อมูลข่าวสารส่วนบุคคลนี้โดยตรงอย่างจริงจัง การยกร่างกฎหมายเกี่ยวกับการคุ้มครองข้อมูลข่าวสารส่วนบุคคล ซึ่งดำเนินการโดยสำนักงานคณะกรรมการข้อมูลข่าวสารของราชการในปัจจุบัน จึงเป็นการดำเนินการที่ตอบสนองความต้องการของสังคมโดยแท้

อย่างไรก็ตาม มาตรการทางกฎหมายและการดำเนินการบังคับใช้กฎหมาย ยากที่จะสัมฤทธิ์ผล หากมิได้มีการเสริมสร้างความรู้ความเข้าใจและการสร้างความตระหนักและเสริมสร้างจิตสำนึกในเรื่องสิทธิความเป็นส่วนตัวและการคุ้มครองข้อมูลส่วนบุคคล จึงจะต้องพัฒนาและเสริมสร้างจิตสำนึกและความตระหนักของสังคม (Public Awareness) แก่เจ้าหน้าที่ของรัฐและแก่ประชาชนควบคู่ไปกับการใช้มาตรการทางกฎหมาย.