BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi yang pesat sejalan dengan berkembangnya peradaban digital dan Indonesia bukan lah pengecualian. Digitalisasi yang menjadi keniscayaan pun menuntut pemerintah untuk mengembangkan berbagai kebijakan digital. Ironisnya, dorongan digitalisasi tersebut tidak diikuti kebijakan keselamatan siber yang menyeluruh bagi anak. Walaupun wacana publik digital terkait aktivitas problematik siber anak menegaskan adanya kondisi yang dilematis dalam kehidupan digital anak, tetapi pemetaan kebijakan keselamatan siber anak masih belum dapat menjamin keamanan anak secara komprehensif. Padahal anak memegang peranan krusial dalam peradaban digital yang sudah mulai terbentuk, terutama mengingat keselamatan anak dalam aktivitas digital mereka berhubungan dengan terpenuhinya hak-hak digital mereka untuk dapat hidup dengan sejahtera di era ini.

Keselamatan siber dalam penerapan digitalisasi sektor pemerintahan di Indonesia, Kota Semarang pada khususnya, menjadi urgensi di era digital. Apalagi rasa aman para pengguna menjadi salah satu tantangan terbesar dalam keberlanjutan peradaban manusia di tengah digitalisasi (Osburg & Lohrmann, 2017). Tidak hanya kalangan dewasa, anak-anak pun patutnya harus aman dalam akses maya yang mereka lakukan sehari-hari. Walaupun

begitu, nyatanya eksistensi kejahatan digital terhadap anak terus ada – semakin lama justru semakin meningkat, terus langgeng dalam sisi gelap dunia digital. Hal tersebut yang menjadi sorotan peneliti, seberapa jauh kah keseriusan Kota Semarang menjamin keamanan digital bagi anak-anak yang tinggal di Ibukota Jawa Tengah ini?

Namun, sebelum membahas lebih lanjut, ada dua hal yang perlu disinggung terlebih dahulu untuk memastikan tersampaikannya dasar permasalahan ini. *Pertama*, keselamatan siber (*cyber-safety)* memiliki sekat pembeda dari prinsip keamanan siber (*cyber-security)*. Hal ini sering kali bias dalam diskursus publik, terlebih secara harafiah, baik *safety* maupun *security* dalam bahasa Indonesia memiliki terjemahan yang sama. Keselamatan siber berbicara tentang bagaimana manusia membangun dan merasa aman dalam aktifitas mereka di ruang siber. Sedangkan keamanan siber berfokuskan pada teknologi itu sendiri dan selalu melibatkan kalangan yang ahli di bidang teknologi informasi dalam penerapannya.

Kedua, tentang betapa pentingnya digitalisasi dalam kehidupan kita. Ada beberapa bukti yang kentara menunjukkan bagaimana aspek digital telah melebur dalam kehidupan sehari-hari, yaitu: Organization for Economic Co-operation and Development (OECD) menjadikannya fokus sejak 2010 dengan menerbitkan dokumen "*Recommendations on ICTs and the Environment*"; Global eSustainability Initiative (GeSI) dengan laporan penelitian mereka pada 2008 bertajuk "SMART 2020"; dan Electronics-Tool for Accountable Supply Chains (e-TASC) yang membantu pengukuran performa berkelanjutan dari suatu perusahaan (Alvarez-Pereira, 2019). Contoh-contoh

di atas menunjukkan digitalisasi bukan sekedar bicara tentang media sosial dan gadget. Jauh dari itu, ia terus meluas hingga mencakup ke banyak aspek kehidupan.

Lebih lanjut, digitalisasi sudah melebur dengan masa depan manusia (Osburg & Lohrmann, 2017). Layaknya aspek lain dalam kehidupan, keberlanjutan manusia mau tidak mau berhadapan dengan teknologi digital – dari Internet of Things (IoT) hingga *Artificial Intelligence* (AI) (Osburg & Lohrmann, 2017). Keberadaannya menjadi semakin penting dalam hidup manusia.

Untuk perihal internet saja, misalnya, penggunanya di seluruh dunia bahkan mencapai 2.7 milyar pengguna atau 40% dari seluruh populasi manusia (Maskun, Manuputty, Noor, & Sumardi, 2013). Tidak mengagetkan lagi, dengan atau tanpa kita sadari, digitalisasi terserap ke semua aspek kehidupan –lingkungan, ekonomi, dan sosial. Tetapi fenomena ini tidak muncul tanpa kendala apapun, terlebih jika kita tengok dari kacamata pemerintahan.

Ada banyak hal yang menjadi tantangan pemerintah dalam menghadapi era digital yang serba virtual ini, seperti misalnya: *new-risk* yang timbul dari sirkulasi pengetahuan yang semakin tidak terkontrol di era sekarang, senada dengan apa yang disampaikan dalam buku Homo Deus (Harari, 2014), menyebabkan institusi negara kesulitan memprediksi peristiwa ekonomi-sosial berskala nasional; Kemunculan pendekatan *Intergovernmental Cooperation*; Penurunan kepercayaan masyarakat terhadap institusi; *digital-*

gap yang mengakibatkan semakin banyaknya kalangan yang tidak terjamah oleh inovasi kebijakan digital (Osburg & Lohrmann, 2017). Tetapi yang akan mendapatkan sorotan utama dalam penelitian ini adalah *cyber-safety* atau seterusnya akan disebut dengan *keselamatan siber*, termaksud di antaranya keselamatan pengguna dan data yang terus dipermasalahkan hingga detik ini (Osburg & Lohrmann, 2017; Szádeczky, 2010; Von Solms & Van Niekerk, 2013).

Keselamatan siber ini bertujuan untuk memastikan agar semua pengguna internet aman selama berselancar di dunia siber (Vanhee, 2018). Terlebih, dunia kini semakin lama semakin tidak memiliki batas fisik, keamanan berseluncur di dunia maya menjadi hal yang sangat penting dalam peradaban global (Kshetri, 2013). Sekali lagi, jika keamanan siber berkutat pada mesin, maka keselamatan siber ini lebih berfokus pada manusianya.

Realita dunia maya yang tidak mempedulikan identitas pengguna, membawa ancaman tersendiri. Hal ini menyebabkan banyak penduduk virtual memilih hadir sebagai *anonymous* –tanpa identitas (Osburg & Lohrmann, 2017). Hal ini tentu memberikan dampak positif dan negatif. Dalam aktivitas siber anak-anak, kondisi ini menimbulkan ancaman yang sangat besar –secara ekstrem bahkan mengerikan.

Anak-anak adalah kalangan rentan dalam banyak kajian kebijakan digital, karenanya perlu perhatian khusus dari pemerintah (Eun Choi, de Guzman, & Singh, 2017; Graafland, 2018; Martin & Rice, 2012). Mereka masih muda dan belum dapat mengklasifikasikan suatu hal berdampak baik atau tidak.

Sebagai contoh, berikan saja anak 5 tahun sebuah permen lollipop, maka anak itu dapat dirayu untuk melalukan apa pun. Ungkapan itu bukan sekadar analogi, tetapi modus yang acap kali diterapkan pada kejahatan terhadap anak *on/offline* –disebut dengan *grooming*[1] (The National Child Traumatic Stress Network, 2009). Baik tidaknya memang tergantung individu dewasa yang terlibat dalam skenario tersebut. Tetapi, kembali ke konteks diskusi, apa yang akan terjadi ketika sosok itu *anonymous*[2] dan berada di dunia maya yang sulit terkontrol? Anak tadi bisa saja belum merasakan dampaknya saat itu juga, tetapi di dunia digital jejaknya ada sebagai hiburan kaum dewasa –secara seksual maupun komersial.

Anak-anak belum dapat lepas sepenuhnya dari jeratan kejahatan siber, mulai dari *online-pornography* hingga jual beli anak. Berapa puluh ribu video *child-porn* dalam situs 'terlarang'? Anda bisa melihatnya hanya dengan bantuan VPN, semudah itu. Begitu saja cukup untuk menutup argumen yang ingin menyanggah betapa gelapnya dunia digital terhadap anak-anak. Miris? Tentu saja. Sayangnya, semua risiko itu terjadi secara global di bawah jejaring internet yang tanpa batasan.

Keselamatan siber pada anak atau *children's cyber-safety* bicara perihal memberikan rasa aman terhadap anak-anak dari ancaman dunia maya. Istilah ini bukan secara kaku bernaung pada satu prasa, *online children safety* a.k.a *child online safety* juga menyimpan makna serupa. Jika sudah timbul rasa aman, maka anak akan dapat merasakan aktivitas dunia maya yang sehat.

[1] Kegiatan membujuk anak-anak, biasanya dilakukan oleh predator anak dalam melancarkan aksi eksploitatifnya.
[2] Hadir tanpa identitas sesungguhnya di dunia siber

Tentunya juga akan berdampak positif pada kehidupan mereka di dunia nyata. Tetapi, sayangnya, realita tidak berbunyi demikian.

Penelitian ini mengulik wacana publik digital terkait aktivitas siber problematik anak untuk memahami kondisi dan permasalahan yang mengancam keselamatan anak, terutama di Kota Semarang. Dari banyaknya isu terkait aktivitas siber anak, penelitian ini berfokus pada tiga isu utama: pornografi online anak, *cyber-bullying* dan kecanduan internet. Ketiga kegiatan problematik tersebut tidak secara mendadak menjadi sebuah isu dan masuk ke dalam ranah diskusi publik.

Popularitas ranah siber yang meningkat hingga detik ini memberikan dampak pada meningkatnya kejahatan siber. Secara global, angkanya ternyata cukup mencengangkan. Internet Watch Foundation (IWF), pada tahun 2016 memaparkan bahwa setiap lima menit seseorang mengakses *webpage* dan setiap sembilan menit *webpage* tersebut menunjukkan konten eksploitasi seksual pada anak. IWF sendiri pada 2016 berhasil mendeteksi 57,335 *webpage* dan 2,416 *domain worldwide* yang mengandung gambar atau video eksploitasi seksual anak, angka ini meningkat 21% dari tahun 2015 (Internet Watch Foundation, 2016).

Tetapi bukan berarti Indonesia mendapatkan keistimewaan untuk bebas dari risiko tersebut, hanya karena dunia digital tidak mengenal teritori fisik. Justru, kasus terkait kejahatan siber yang berkaitan dengan anak-anak di Indonesia angkanya terus meningkat. Hal tersebut terbukti dari studi yang dilakukan oleh Badan Penelitian dan Pengembangan Sumber Daya Manusia

Kementerian Komunikasi dan Informasi berjudul “Digital Citizenship Safety among Children and Adolescents in Indonesia” menyebutkan bahwa setidaknya 30 juta anak-anak dan remaja di Indonesia merupakan pengguna internet dan media digital saat ini menjadi pilihan utama saluran komunikasi yang mereka gunakan. Tak hanya berhenti disitu, 14% diantaranya beberapa kali mengakses konten pornografi dan 52% pernah melihat konten pornografi. Sedangkan 58% anak-anak tidak sadar mengenai adanya *cyber-bullying*, sisanya yang sadar (sebanyak 42%) terdapat 13% di antaranya yang menjadi korban (Gayatri et al., 2015). Tak berhenti disitu, ECPAT (End Child Prostitution in Asian Tourism) mengungkapkan dalam rentang tahun 2011-2014, terjadi 186 kasus terkait prostitusi online anak-anak di Indonesia –dan terus bertambah setiap tahun.

Data statistik di atas tentu tidak memberikan perasaan lega. Ditelaah lebih dalam, digitalisasi yang terus didorong oleh pemerintah menjadi tanda tanya besar dalam aplikasinya di Indonesia. Berbagai daerah berlomba-lomba menjadi ‘*smart’*, dari perkotaan hingga perdesaan. Tetapi, Indonesia hingga kini terkesan enggan meletakan anak-anak di posisi penting yang rentan terhadap sisi gelap ruang siber, baik dari segi kebijakan hingga regulasi (Khairunnissa, Rahman, Siregar, Tanjung, & Shawal, 2018).

Di Kota Semarang, perihal keselamatan siber pada anak masih sedikit dibahas dalam riset-riset sebelumnya. Tetapi, ada baiknya jika kita tetap mengungkit sedikit penelitian yang setidak-tidaknya menyinggung perihal kekerasan terhadap anak-anak di Ibukota Jawa Tengah. Pada tahun 2012 saja

angkanya mencapai 1474 kasus, meliputi kekerasan fisik, psikis dan seksual (Andriyanto & Purnaweni, 2017).

Penting pula untuk meneliti peranan institusi baik pemerintah maupun non-pemerintan atau LSM dalam memastikan keselamatan siber di Kota Semarang. Bagaimana pun, pemerintah memiliki kewajiban untuk memastikan keamanan warganya di dunia nyata maupun maya, anak-anak maupun dewasa. Walaupun begitu, hingga detik ini kepentingan kalangan 'dewasa' selalu lebih menerima sorotan, katakanlah pertumbuhan ekonomi yang bagaikan kiblat pemerintah Indonesia dari merdeka hingga detik ini. Hal tersebut mungkin saja terjadi di Kota Semarang, tetapi bisa jadi tidak –untuk itulah penelitian ini dirancang.

Mengetahui pentingnya memecahkan permasalahan ini, maka peneliti kemudian menyusun strategi penelitian kualitatif dengan menerapkan pendekatan studi kasus. Sedangkan, data yang dibutuhkan untuk memperkuat kesimpulan didapat melalui wawancara tatap muka dengan narasumber terkait. Melalui proses tersebut, kemudian diharapkan hasil penelitian ini dapat menerangkan mengenai keselamatan siber pada anak di Kota Semarang.

1.2 Perumusan Masalah

Mengingat bahwa masa depan bukan hanya milik insan saat ini dan di saat bersama digitalisasi mulai merambah ke berbagai sektor kehidupan, maka memang anak-anak seharusnya mendapat perhatian lebih besar dalam kegiatan maya mereka sehari-hari. Tetapi realita di lapangan, berdasarkan

statistik nasional dan regional terkait kasus kejahatan digital terhadap anak, menunjukkan hal yang sebaliknya.

Berdasarkan hal itu, beberapa pertanyaan penelitian yang diharapkan dapat membantu menemukan kejelasan terkait keselamatan siber di Kota Semarang dapat dirumuskan sebagai berikut:

Bagaimana kebijakan keselamatan siber anak di Kota Semarang?

Untuk menjawab pertanyaan tersebut, ada hal utama yang perlu mendapat kejelasan terlebih dahulu, yaitu: ***Bagaimana wacana publik digital di Kota Semarang terkait aktivitas siber problematik anak?***

Perihal pertama tersebut penting untuk dipecahkan terlebih dahulu, karena kurangnya literasi yang spesifik mengarah ke Kota Semarang.

Kemudian, perihal yang kedua muncul ketika penulis menyadari bahwa keselamatan siber pada anak tidak dapat dijamin dengan kebijakan pemerintah semata, walaupun regulasi yang kuat juga sangatlah penting. Peneliti menyadari bahwa NGO/LSM juga memegang peranan tidak kalah berharganya. Sehingga, peneliti menggunakan istilah institusi –bukan hanya menyoroti pemeritah semata.

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk memetakan bagaimana institusi di Kota Semarang, baik pemerintah maupun NGO/LSM, melakukan keselamatan siber pada anak. Di saat bersamaan, peneliti juga memiliki tujuan untuk membuka wawasan umum bahwa ada bahaya dari dunia maya terhadap anak-

anak. Peneliti menyadari bahwa hingga detik ini hal tersebut belum mendapat posisi penting dalam pandangan publik, dibandingkan permasalahan lain seperti korupsi. Terlebih, karena keberadaannya di ‘sisi gelap’ ruang siber, menyebabkan kasus ini menjadi licin untuk diketahui publik.

1.4 Manfaat Penelitian

1.4.1 Manfaat Teoritis

Dengan dilakukannya penelitian ini diharapkan dapat memperkaya khazanah keilmuan, terutama dalam bidang studi ilmu politik pemerintahan, terkait peranan institusi dalam menjamin keselamatan siber.

1.4.2 Manfaat Praktis

Menambah literasi publik terkait konteks *children cyber-safety* di Indonesia dengan spesifikasi di Kota Semarang. Di saat bersamaan, penulis akan mencoba meramu ancaman-ancaman digital terhadap anak di era digitalisasi dengan kebaruan yang ringan tanpa mengurangi substansi-nya agar menjadi pertimbangan bagi parenting maupun pembuat kebijakan siber kedepannya.

1.5 Literature Review

Buku bertajuk *Sustainability in a Digital World: New Opportunities Throught New Technologies* menjadi pemantik utama dan pertama dari dilakukannya penelitian ini, karena buku ini memberikan pemahaman terkait digitalisasi dalam kehidupan berkelanjutan manusia. Ditulis pada 2017 oleh

banyak penulis berbeda untuk setiap *chapter*-nya, buku ini menyajikan kajian yang peneliti anggap cukup luas untuk dapat memahami problem dan kesempatan dari era digitalisasi. Seluruh isi buku ini mudah dipahami, walau konteks pembahasannya sedikit berat –terutama bagi peneliti, terlebih ketika memasuki *chapter* dengan banyak istilah ilmiah teknis. Tetapi, bukan berarti buku ini lepas dari bidang keilmuan humaniora –pemerintahan pada khususnya.

Setidaknya, ada dua *chapter* penting dari buku di atas yang masuk ke dalam *literature review* kali ini. Pertama, *Sustainability in a Digital World Needs Trust* yang ditulis oleh Thomas Osburg. Pada *chapter* ini, Osburg memaparkan beberapa hal penting yang membentuk pemahaman terkait keberlanjutan dunia digital. Ia menegaskan ada hubungan erat antara transformasi digital dan *sustainability*, walau tidak secara langsung dideklarasikan. Kemudian Osburg juga memecah pembahasan terkait digitalisasi ke dalam tiga aspek dasar kehidupan berkelanjutan, yaitu: ekonomi, lingkungan, dan sosial. Di sini lah, penulis menegaskan bahwa digitalisasi berpengaruh sangat besar pada aspek sosial dari kehidupan yang berkelanjutan. Hal ini senada dengan apa yang disampaikan oleh Al Gore dalam *Earth in the Balance* –tentang *climate crisis* serta peranan manusia di dalamnya, dan Harrari di bukunya Sapiens dan Homo Deus. Tetapi, inti dari tulisan Osburg tidak berhenti disitu.

Argumen utama Osburg mengenai keberlanjutan manusia di era digital adalah terkait krisis kepercayaan dan *digital-gap*. Kesenjangan digital ini muncul ketika banyak orang tidak mendapatkan pemahaman yang cukup

untuk bersanding dengan golongan masyarakat berpendidikan yang telah terpapar digitalisasi. Kesenjangan ini lah yang menyebabkan munculnya masyarakat yang tertinggal dari akses kebijakan digital (Osburg & Lohrmann, 2017). Hal ini lah yang kemudian menyebabkan kepercayaan menjadi turun, terutama yang berhubungan dengan institusi. Terjun payung-nya kepercayaan terhadap institusi inilah yang kemudian membawa kita melompat pada *chapter* kelima yang bertajuk: *Sovereign Decisions as a Means for Strengthening Our Resilience in a Digitalized World*.

Chapter yang ditulis oleh Denise Feldner ini menyampaikan mengenai beberapa hal terkait ketahanan digital di banyak negara. Tulisan ini secara keseluruhan tidak begitu menyentuh perihal politik-pemerintahan. Ia menggaris bawahi istilah digitalisasi sebagai tantangan terbesar masa kini dan secara langsung berkaitan dengan aspek: 1) *security*, 2) ekonomi, dan 3) masyarakat (Osburg & Lohrmann, 2017). Kemudian, Faldner memfokuskan kajiannya pada keamanan digital, terutama dengan menjadikan German sebagai contoh dari negara yang sangat memprioritaskan keamanan digital-nya. Dari analisisnya ini, peneliti kemudian menemukan bahwa keamanan digital menjadi sangat penting dan bukan hanya tanggungan internasional. Hal terkait atas privasi dan keamanan digital menyentuh langsung ke kehidupan masyarakat. Jika sudah begitu, semakin jelas lah bahwa *digital-security* menyangkut kebijakan politik yang bersifat domestik.

Dari artikel ini, peneliti menemukan beberapa pertanyaan. Siapa saja masyarakat yang berpotensi mengalami *digital-gap*? Apakah keamanan siber hanya berhenti pada keamanan data penduduk? Bagaimana pemerintah

menjamin data penduduk tetap aman? Setelah melanjutkan pencarian dan pengkajian literatur dengan lebih mendalam, akhirnya peneliti mendapatkan jawaban untuk semua pertanyaan di atas.

Untuk pertanyaan terkait siapa saja masyarakat yang rentan mengalami *digital-gap*, sebenarnya ada banyak jawaban. Tetapi, anak-anak langsung masuk ke dalam perhatian peneliti karena memberi kesan ironi tersendiri. Mereka adalah kalangan masyarakat yang dari lahir sudah terpapar digitalisasi, tetapi justru menerima risiko yang lebih besar dari kalangan usia lainnya. Jawaban ini dipertegas ketika peneliti memasuki *chapter* berjudul *The Risk Averse Society: A Risk for Innovation?* –masih dari buku yang pertama.

Pertanyaan kedua mendapat jawaban ‘tidak’ ketika peneliti menemukan bahwa keamanan digital melingkupi keamanan dari *hardware* dan *software* digital. Kemudian keamanan digital muncul dalam proses pengkajian peneliti sebagai wujud pengamanan dunia-maya, berikut juga mengekor istilah seperti *cyber-crime, cyber-safety, cyber-troop*, dan sebagainya.

Literatur berikutnya adalah *Safeguarding cyborg childhoods: Incorporating the on/offline behavior of children into everyday social work practices* yang merupakan hasil riset dari Corinne dan kawan-kawan, muncul untuk mempertegas posisi penting dari ‘anak-anak’ untuk konteks terkait keamanan siber. Dalam jurnal ini, mereka melakukan riset terkait aktivitas anak-anak dalam ruang siber, terutama tentang cara anak-anak

mengidentifikasi orang asing ketika berkecimpung di CMC (*computer-mediated communication).*

Mereka pun menemukan bahwa anak-anak yang lahir di era digitalisasi dapat dikatakan sebagai *cyborg* karena cara mereka memindai lawan komunikasi di dunia maya sudah seperti mesin. Mereka membandingkan ada kemiripan diantara keduanya (May-Chahal et al., 2014). Tetapi, berbeda dengan mesin, anak-anak masih memindai orang asing ketika melakukan CMC dengan cara yang sangat tidak efektif (May-Chahal et al., 2014). Dari jurnal ini, peneliti menemukan bahwa anak-anak sudah tidak terpisahkan dari dunia maya, sehingga penting memastikan mereka aman dalam aktivitas *online* mereka. Tetapi jurnal ini masih meninggalkan beberapa celah terkait tindak-lanjut dari cara anak-anak memindai orang asing di dunia maya. Bagaimana peran orang tua, guru, dan institusi terkait untuk menjamin keamanan anak dalam konteks terkait?

Celah dari jurnal di atas membawa peneliti kepada jurnal berjudul: *Long-term study of safe Internet use of young children.* Riset kali ini menggali perihal hubungan antara penggunaan internet anak-anak dan kontrol orang tua. Menjadi penting, terlebih peneliti sempat bertanya-tanya mengenai peran orang tua dalam memastikan keamanan berselancar-maya anak-anak, sebelum mempertanyakan peran institusi. Kemudian, penelitian ini menerangkan bahwa ternyata kontrol orang tua dan guru terkait penggunaan internet oleh anak-anak menurun drastis pasca tahun 2005 (Valcke, De Wever, Van Keer, & Schellens, 2011). Tetapi, penelitian ini justru mendorong peningkatan peran orang tua ketimbang regulasi belaka. Karena, menurut

mereka, penegakan hukum kurang efektif untuk menjamin keamanan anak di dunia maya. Mengetahui hal ini, peneliti merasa perlu melakukan klarifikasi untuk memastikan temuan tersebut.

Ternyata, jurnal lainnya yang berjudul, '*Children's cyber-safety and protection in Australia: An analysis of community stakeholder views'* memberikan klarifikasi dibalik argumen kurang efektifnya regulasi dalam menjamin keamanan anak di dunia maya. Jurnal yang ditulis oleh Nigel Martin dan John Rice ini menggali keamanan ruang siber bagi anak-anak dari perspektif *stakeholder* di Australia. Membaca temuan dalam jurnal ini membuat peneliti sadar bahwa penegakan hukum perihal keselamatan dunia maya bagi anak-anak akan lebih efektif ketika suatu negara sudah memiliki regulasi yang jelas dan komprehensif terkait hal itu.

Australia, misalnya, memiliki regulasi yang jelas untuk menjamin peran orang tua dalam memandu penggunaan internet anak-anaknya (Martin & Rice, 2012). Sehingga kemudian, ketimbang mengubah regulasi, menurut jurnal ini, Australia lebih memerlukan dorongan untuk memperkuat edukasi terhadap orang tua dan komunitas masyarakat terkait konteks keselamatan siber kepada anak-anak. Selain temuan itu, peneliti juga menyadari bahwa kedua jurnal tersebut memiliki relevansi mengingat penelitian pada sumber sebelumnya berada di Inggris dan Australia pun negara perserikatan Inggris.

Kemudian, bagaimana dengan Indonesia? Apakah regulasi terkait keamanan anak di dunia digital di Indonesia sudah jelas?

Pertanyaan tadi membawa peneliti kembali kepada Merlyna Lim yang fokus kajiannya adalah tentang *digital movement* di Asia Tenggara. Sayang, tidak ada satu pun jurnal Lim yang secara spesifik menyoroti anak-anak dan keamanan mereka ketika beraktivitas di dunia maya. Tetapi setidaknya, dalam artikelnya yang bertajuk *The Internet and Everyday Life in Indonesia: A New Moral Panic*, Lim menyinggung *online child-porn*. Dalam artikel yang sama pula, Lim me-*review* 11 buku terkait *cyber-porn*. Ia berhasil menguraikan secara gamblang banyak hal terkait *pornography* dunia maya yang tabu, tetapi disenangi di Indonesia (Lim, 2013). Dari sejarah hingga regulasi pemerintah untuk menangani kejahatan digital.

Celah yang belum banyak disinggung oleh Lim tersebut lantar mengantarkan peneliti pada jurnal lainnya yang bertajuk: "*The Phenomenon Of Cyber Crimes Which Impact Children As Victims In Indonesia"* yang ditulis oleh Hardianto Djanggih pada Mei 2018. Jurnal ini mengulas kejahatan dunia maya yang berdampak pada anak-anak dari perspektif kriminologi. Temuan dalam jurnal ini cukup mengejutkan. Salah satu diantaranya, yang paling mengejutkan peneliti, ketika ia menyatakan bahwa anak-anak juga korban dari *phytophilia*[3].

Kemudian, ia juga memaparkan jenis-jenis kejahatan siber yang melibatkan anak sebagai korban, yaitu meliputi: *cyber-porn*, *cyber-bullying*, *online-fraud*, dan kejahatan lainnya (Djanggih, 2018). Beberapa teori masuk ke dalam analisis Djanggih untuk menjelaskan fenomena kriminal *online*, terutama yang melibatkan anak-anak sebagai korban, seperti teori kontrol

[3] Kegiatan seksual dengan tumbuhan

sosial dan kontrol individu. Ia juga menegaskan bahwa penguatan regulasi terkait konteks kejahatan digital terhadap anak harus lebih diprioritaskan. Tapi, tunggu dulu, memangnya bagaimana regulasi pemerintah terkait hal tersebut?

Cyber-security Policy and Its Implementation in Indonesia memberikan penjelasan terinci terkait perundangan yang mengatur perihal keamanan siber. Regulasi yang ada selama ini hanya mengatur konten negatif atau pornografi yang terdapat dalam UU No. 44 tahun 2008 tentang Pornografi dan UU No. 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik. Sebenarnya terdapat banyak regulasi menyangkut *cyber*-security di Indonesia, tetapi mayoritas berkutat pada perhiral keamanan dan ketahanan negara(Rizal & Yani, 2016). Tetapi tidak ada satu pun dalam regulasi tersebut yang mengatur secara jelas dan komprehensif terkait keamanan anak-anak di dunia maya. Sehingga, peneliti pun memahami bahwa, memang, dibandingkan agenda regulasi digital lainnya, keselamatan siber kepada anak-anak tidak mendapat perhatian utama.

Setelah mengaji jurnal di atas, peneliti kemudian berusaha membandingkan regulasi Indonesia terkait keselamatan anak di dunia digital dengan negara-negara tetangga. Hal ini lah yang membuat *Mapping Online Child Safety In Asia And The Pacific* masuk ke dalam *literature review*. Riset ini memetakan bagaimana negara-negara di Asia dan Pasifik menanggapi keamanan anak di dunia siber. Dalam jurnal ini, Indonesia di kelompokan dalam kategori *low internet penetration* –walau pun berpotensi besar untuk

terus meningkat. Di banding Indonesia, Malaysia dan Vietnam ternyata jauh lebih peka dalam konteks keamanan anak di Internet. Begitu juga Australia dalam penanganan *cyber-bullying* kepada kalangan anak-anak, Korea dengan regulasi yang mengatur kecanduan dalam menggunakan gadget bagi anak, bahkan Jepang dengan regulasi mengatur konten berbahaya (Singh, 2018). Dari riset ini, jelas Indonesia sebenarnya harus kejar ketertinggalan terkait regulasi yang melindungi anak-anak dari bahaya dunia maya –berhubung penetrasi internet-nya masih tergolong rendah.

Demikian *literature review* di atas merangkai logika peneliti dalam meramu penelitian ini. Total ada tujuh jurnal dan satu buku yang berkontribusi menjadi landasan pemikiran peneliti. Sehingga semakin jelas lah bahwa masalah keselamatan anak di dunia siber perlu dipertanyakan untuk menjamin terbentuknya masyarakat yang berkelanjutan di era digital.

1.6 Kerangka Pemikiran Teoritis

1.6.1 Teori Wacana

Teori Wacana mulai dikenal pada akhir 1970-an, terutama distimulus oleh meletusnya peristiwa Mei 1968, perdebatan kritis mengenai paham strukturalis, hingga krisis Marxism dalam menghadapi neoliberal dan hegomoni konservatif (Torfing, 2004). Pengembang teori ini pun beragam, mulai dari Habermas hingga Foucault.

Dalam perkembangannya, menurut Torfing (2004, 6-8) teori wacana dibagi ke dalam tiga generasi, iaitu:

a. Generasi Pertama: teori wacana hanya berkisar pada lingkup sempit diskursus linguistik dan berfokus pada aspek sematik dari ucapan maupun tulisan. Tetapi, tidak ada usaha yang kentara untuk menghubungkan antara analisis wacana dan pertentangan politik.
b. Generasi Kedua: Menjadi semakin luas, teori wacana tidak lagi seputar ucapan dan tulisan. Melainkan, melebar hingga ke banyak aspek fenomena sosial. Terima kasih kepada Foucault yang meramu teori wacana menjadi kumpulan praktis yang empiris yang dapat diwacanakan asalkan memiliki unsur kesamaan (Foucault, 1972). Bersamaan dengan itu, teori wacanapun merambah ke komunikasi tidak tertulis dan tidak verbal –dari gambar hingga gestur. Tetapi kemudian, Hebermas berusaha menghilangkan aspek politik dan kekuasaan dalam teori yang dikembangkan Foucault. Mengingat, Foucault meracik teori yang kental dengan adanya relasi kekuasaan dan politik.
c. Generasi Ketiga: Kemudian, teori wacana kembali berkembang hingga mencakup seluruh fenomena sosial. Wacana bukan menjadi hal khusus, tetapi meliputi ilmu sosial lainnya. Menyebabkan perkembangan ilmu sosial menjadi terpartisi.

Terkait diskursus atau wacana, misalnya mengenai kebijakan, terdapat beberapa langkah yang saling terhubung untuk memastikan hasil temuan dalam penelitian. *Pertama,* Problemalisasi yang mengkonstrak objek permasalahan dalam penelitian. *Kedua,* retroduksi yang menjadi langkah untuk merangkai hipotesis berdasarkan pre-riset sebelum penelitian. Lalu, logis yang merasuki penjelasan dalam analisis. Kemudian, artikulasi yang

mengoneksikan hasil analisis. Terakhir, kritik untuk menutup yang biasanya berwujud pada garis besar relasi dan dominasi terkait analisis yang telah dikoneksikan tadi.

Dalam penelitian ini, teori wacana yang digunakan berpusat pada pemikiran Foucault. Karena, sangat cocok digunakan untuk mengekspos banyak hal penting dari kebijakan keselamatan anak di Semarang. Foucault juga tidak memberi batas kepada interpretasi pembaca terkait buku-bukunya seputar teori wacana. Tetapi, setidaknya, dalam bukunya yang berjudul Archeology of Knowledge, Foucault menegaskan bahwa wacana yang dimaksud digunakan untuk menelaah apapun, bahkan yang tertulis dan tidak tertulis, terucap dan tidak terucap. Karenanya, di dalamnya termaksud gambar, symbol, gestur, video maupun permainan. Dari sini, kita akan masuk ke dalam wacana digital.

1.6.1.1 Wacana Digital

Seiring berkembangnya teknologi digital, tidak mungkin Teori wacana tetap seperti dahulu. Wacana digital muncul sebagai turunan teori wacana, membawa formula baru sebagai perspektif analisis yang memang diperuntukan untuk riset mengenai komunikasi digital (Jones, 2015).

Munculnya dunia digital tentu memperluas jangkauan komunikasi, begitu juga dengan wacana atau diskursus yang berkembang di dalamnya. Di tengah komunikasi dengan media komputer yang terus berkembang, teori wacana kini juga menjalar ke banyak media. Mulai dari teks, chat, komentar, *caption*, video hingga permainan (Insights & Directions, 2019; Thurlow & Mroczek,

2012). Walaupun, memang, wacana digital berbagi kemiripan dengan isu-isu pada *metalanguage* serta ideology dalam bahasa, tetapi fokusnya adalah pada media baru yang kontemporer (Thurlow & Mroczek, 2012).

Dalam praktik riset, menurut Jones (2015, 7-10), wacana digital dapat dianalisis dengan memperhatikan empat aspek, iaitu:

a. Teks: bagaimana bedanya studi penulisan menggunakan teknologi yang mambuat kita dapat menggabungkan unsur-unsur sematik menjadi bentuk yang dapat dipahami masyarakat yang juga mempengaruhi perilaku di komunitas.
b. Konteks: sosial atau situasi sosial yang memkontruksi sebuah teks, dikonsumsi, bertukar-tukar dan diperbolehkan untuk diterima publik.
c. Aksi dan interaksi: apa orang-orang lakukan dengan teks, terutama apa yang mereka lakukan satu sama lain.
d. Kekuasaan dan ideologi: Bagaimana orang menggunakan teks untuk mendominasi dan mengontrol orang lain dan menyiptakan ‘versi lain dari kenyataan’ tertentu.

Keempat aspek tersebut dipengaruhi oleh teknologi apa yang digunakan dalam berkomunikasi atau meramu wacana. Jika menggunakan android, *User Interface* (UI) dan fitur di dalamnya juga patutnya dipertimbangkan dalam analisis. Demikian pula dengan konteks atau isi dari pesan yang disampaikan, baik melalui teks atau bahkan permainan online. Lalu, terkait dengan aspek ke empat, maka jelas memang teori Foulcault tentang wacana berpengaruh

besar. Iaitu tentang bagaimana *netizen* menggunakan media baru untuk mendominasi dan mengontrol pengguna lainnya.

1.6.2 Keselamatan Siber

Keselamatan siber atau *cyber-safety* merupakan perpaduan antara *cyber-security* dan *industrial Safety*. Adapun tiga roda dari budaya keamanan terdiri atas: *zero incident*, pelaporan dari peristiwa berpotensi menimbulkan kecelakaan atau kerugian sebelum benar-benar terjadi, dan ABC *(behavioral analysis)* (Borilin, 2014). Definisi lain merujuk *cyber-safety* sebagai situasi sempurna dimana setiap individual beraktivitas di *cyber-space* dengan rasa aman dan bertanggungjawab dengan penggunaan *information and communication technologies* (ICT) (Vanhee, 2018).

Terdapat beberapa sektor yang terlibat dalam keselamatan siber, salah banyaknya adalah pemerintah, institusi penegak hukum, keluarga, perusahaan, non-government organization (NGO), hingga teman sepergaulan (Martin & Rice, 2012; Von Solms & Von Solms, 2015).

Salah satu cara untuk menjamin rasa aman dalam berselancar di dunia maya. Pertama, *encryption* yang merujuk pada proses pengubahan bentuk (*encoding)* dari pesan atau informasi yang hanya pihak-pihak berwenang saja yang dapat membacanya. Hal ini perlu untuk menjamin keamanan dari komunikasi yang dilakukan. Beberapa media sosial mengedepankan *encryption* untuk menjamin privasi pengguna, misalnya:Telegram dan Whatsapp. Beberapa kelompok peretas pun mengeluarkan *platform*

berkomunikasi dengan keamanan yang jauh lebih terjamin, seperti: Signal dan Wickr Me.

Namun, *encryption* ini juga dapat menjadi ancaman. Karena, dengan pengamanan yang sangat baik untuk menjamin pengguna lepas dari penyadapan dan pemantauan, media itu dapat menjadi tempat bertransaksi konten-konten ilegal (Singh, 2018). Selain itu, *e-currency* juga membawa problem tersendiri terkait paradox dalam penggunaannya. Demikian pula *deep web* yang juga memberikan ancaman tersendiri. *Deep web* tidak dapat diakses melalui laman *browser* biasa, begitu juga alat pencarian digital biasa. Setiap pengguna yang mengakses *deep web* adalah anonymous yang menutup identitasnya dengan baik, biasanya menggunakan *The Onion Router* (TOR). Jauh lebih tidak tersentuh lagi adalah *dark web* yang menjadi tempat berselancar transaksi illegal seperti senjata, narkoba, dan sebagainya (Vanhee, 2018).

Sehingga, pada akhirnya *cyber-safety* adalah pencegahan sebelum potensi bahaya di dunia *cyber* terpapar ke masyarakat yang rentan. Dalam konteks ini, anak-anak menjadi kalangan yang paling rentan. Sehingga keamanan siber terhadap anak-anak mendapat sorotan prioritas di kancah global. Tetapi sebenarnya apakah itu?

1.6.3.1 Keselamatan Siber Kepada Anak-Anak

Istilah keselamatan siber untuk anak-anak merujuk pada hal yang sama dengan istilah *child Safety Online* –yang digunakan oleh Unicef. Keduanya

mengarah pada upaya perlindungan anak dari risiko yang ditimbulkan dari dampak negatif lingkungan siber (Martin & Rice, 2012).

Risiko yang ditimbulkan dari interaksi *online* kalangan anak-anak dapat dibagi menjadi tiga jenis, menurut A.R. Mubarak yang dikutip dari Jurnal berjudul *Mapping Online Child Safety in Asia-Pacific* (Eun Choi et al., 2017), seperti berikut:

a. Konten

Jenis konten yang ditemui anak-anak bisa jadi tidak pantas, berpotensi bahaya dan ilegal. Seperti *website* yang mengampanyekan *self-harm*, *hate-speech* dan pornografi. Konten tersebut dapat mempengaruhi anak-anak untuk melakukan dan berhubungan dengan aksi-aksi berisiko dalam kehidupan nyata, seperti ekspoitasi seksual.

b. Penggunaan/Tingkah laku

Bagaimana anak-anak menggunakan internet bisa jadi berisiko bagi mereka. Hal tersebut juga termaksud konten-konten yang dibuat oleh anak-anak itu sendiri. Risikonya dapat berupa *cyber-bullying*, *sexting*, transaksi penipuan, dan hal-hal lainnya yang menyangkut privasi dan keamanan –juga kecanduan internet.

c. Interaksi/Komunikasi

Interaksi dengan individu-individu, terkhusus melalui media sosial dan ruang *chat*, dapat memperbesar kemungkinan anak-anak bersinggungan dengan *online grooming* dan janjian untuk bertemu orang asing yang eksploitatif.

Dari penjabaran di atas, maka kita dapat mengetahui beberapa jenis yang secara spesifik berisiko besar membahayakan anak-anak. Dari kesemuanya itu, ada beberapa hal yang menjadi perhatian mayarakat global dan khususnya ilmuwan sosial, tetapi yang paling banyak mendapat sorotan adalah *child cyber-porn*, *cyber bullying* dan kecanduan/ketergantungan internet.

1.6.3.1.1 Pornografi siber anak

Istilah ini memiliki kesamaan makna dengan *online child sexual abuse* atau juga *child pornography. The Scope and Magnitude of Online child sexual abuse in Indonesia* yang diterbitkan oleh ECPAT Indonesia memaparka bahwa *child cyber-porn* adalah tindakan kriminal yang melanggar norma kesopanan yang menggunakan teknologi informasi sebagai media untuk mengomunikasikan, menunjukkan dan menyebarluaskan berbagai konten pornografi kepada anak-anak (ECPAT Indonesia, 2012) .

Dari sumber yang sama, Catherine Beaulieu memaparkan bahwa *child cyber-porn* dapat mengeksploitasi anak dengan berbagai cara:

1. Anak-anak mungkin tertipu dan dipaksa mengikuti aktivitas seksual untuk memproduksi konten pornografi atau pun gambar yang mengeksploitasi anak secara seksual tanpa sepemahaman anak tersebut. Konten itu nantinya akan disebarkan atau diperjualbelikan.

2. Permintaan terhadap konten anak tersebut mendorong produksi konten online child sexual abuse. Pemintaan tersebut yang terus menurus menuntut agar eksploitasi seksual terhadap anak terus dilanjutkan.

3. Konten pornografi tersebut sering kali digunakan oleh pelaku pelecehan untuk mengurangi penolakan anak dan menunjukan kesan bahwa kegiatan seksual antara anak-anak dan orang dewasa adalah hal yang normal, dapat diterima dan menyenangkan. Ini adalah bagian dari *grooming*.

4. Konten pornografi tersebut kemudian digunakan pelaku untuk memaksa anak-anak membuat konten serupa.

1.6.3.1.2 *Cyber-bullying*

Cyber-bullying sebenarna sama saja dengan *bullying* yang dilakukan secara tradisional, hanya saja media nya berbasis internet –*social media* misalnya. *Bullying* sendiri merujuk pada perilaku agresif yang tidak diinginkan diantara anak-anak masa sekolah yang melibatkan kekuasaan yang tidak berimbang di dalamnya, meliputi ancaman, penyebaran rumor-rumor, penyerangan secara fisik maupun verbal, pengucilan orang secara sengaja dari suatu kelompok (Fauzia, 2018).

Walaupun dilakukan di *cyber-space*, *bully* jenis ini juga dapat berhubungan dengan kehidupan nyata. Anak-anak yang menghabiskan sebagian besar waktu dengan menggunakan *gadget*, dapat meningkatkan risiko dari *cyberbullying* –baik sebagai pelaku maupun korban. Adapun perempuan lebih sering dijadikan sebagai korban ketimbang laki-laki, tentunya masih dalam usia sekolah . Biasanya, pem-*bully*-an secara *online* ini menjadikan kalangan anak-anak minoritas sebagai korbannya, seperti etnis minoritas, LGBTQ muda, anak-anak dengan berat badan berlebih, dan anak-anak berkebutuhan khusus (UNICEF Innocenti Research Centre, 2011).

1.6.3.1.3 Kecanduan/Ketergantungan Internet

Secara umum kecanduan/ketergantungan internet merujuk pada perilaku obsesif menggunakan internet secara berlebihan yang tidak terkontrol hingga menimbulkan ketergantungan (Huang, Hu, Ni, Qin, & Lü, 2019). Fenomena ini sudah berkembang dengan ironis akibat perkembangan teknologi yang begitu cepat, hingga kemudian menjadi sebuah sindrom yang berdiri dibawah istilah *Internet Addiction Disorder* (IAD) oleh Ivan Goldberg pada 1996 (Fradelos, Kourakos, Velentza, Polykandriotis, & Papathanasiou, 2016).

Kecanduan terhadap internet dapat dibagi ke dalam empat tipe jenis mendasar yang meiputi: 1) *Cyber sexual addiction* (kecanduan terhadap konten seksual di Internet), orang yang mengalami kecanduan jenis ini biasanya berhadapan dengan aktivitas melihat, mengunduh, danmemperdagangkan konten pornografi melalui internet dan berinteraksi langsung melalui ruang *chat* dewasa dengan memainkan 'peran' dalam permainan fantasi; 2) *Cyber-Affair*, meliputi kecanduan bermain dalam forum diskusi maya, mengirim pesan singkat, dan berpartisipasi melalui sosial media berbasis internet; 3) *Net Compulsions*, kecanduan kepada *game online*, perjudian *online*, dan dalam *eBay*; 4)*Information overlaod*, ditimbulkan oleh ketersediaan informasi yang sangat luas di internet, kecanduan dalam bentuk 'berselancar' di dunia maya (Fradelos et al., 2016).

1.7 Operasionalisasi Konsep

Setelah mengkaji literatur dan mengetahui teori yang akan digunakan untuk mempertajam analisis data, peneliti kemudian akan mengelaborasi

terkait operasionalisasi konsep. Adapun sebelum lebih lanjut, peneliti memberikan batasan kepada usia dari kelompok anak yang masuk dalam penelitian ini, yaitu di bawah 18 tahun sesuai dengan UU No. 23 tahun 2002 tentang Perlindungan Anak. Berikut adalah elaborasinya:

1.7.1 Wacana Digital dalam Ruang Siber untuk anak

Wacana digital dalam ruang siber akan menjadi gerbang untuk menarik pembahasan dalam analisis penelitian ini lebh dalam. Wacana digital adalah segala konten digital yang dibuat atau dilakukan oleh anak dalam ruang maya untuk berinteraksi denan pengguna internet lainnya.

Wacana digital yang dimaksud di antaranya melingkupi teks, video, music, dan permainan. Kemudian, perlu juga menarik peran orangtua dalam mengawasi aktifitas anak, gadget tipe apa yang mereka gunakan untuk berselancar di dunia maya.

1.7.2 Keselamatan Siber untuk anak

Meningkatkan keselamatan siber menjadi hal yang penting dalam penelitian ini, terutama dalam upayanya meningkatkan keamanan digital untuk keberlanjutan masyarakat. Dengan keamanan siber dan upaya pencegahan atas kejahatan digital yang mapan, maka keselamatan siber pun dapat dijamin. Hal ini menyoroti berbagai pengamanan atas kejahatan-kejahatan digital yang acap kali terjadi. Dalam penelitian ini, peneliti menyoroti setidaknya dua hal kejahatan digital: *cyber-porn* a.k.a *online-porn*, *cyber-bullying*. Dua kejahatan tersebut dipilih karena ‘popularitas’-nya di Indonesia -dalam konteks negatif.

Cyber-porn, dalam konsep penelitian ini, merujuk pada eksploitasi seksual yang dilakukan dengan teknologi digital. Termaksud juga di dalamnya penggunaan kamera untuk pengambilan konten pornoaksi atau perilaku diluar norma susila yang bersifat seksual, terlebih-lebih transaksi dan komersialisasi konten serupa.

Cyber-bullying, dalam pandangan penelitian ini diklasifikasikan sebagai kejahatan digital yang melibatkan pelecehan, pencemaran serta penindasan yang dilakukan dengan posisi kekuasaan yang tidak berimbang, dilakukan menggunakan media berbasis internet.

Walaupun sebenarnya, *cyber-security* menyangkut hal yang lebih luas dari apa yang telah dielaborasi di atas, seperti *cyber-terrorism*. Tetapi peneliti memfokuskan hanya pada dua hal tersebut mengingat kaitannya dengan konteks anak-anak.

Kemudian, selain mencakup dua kejahatan digital yang sebelumnya telah dijabarkan, *children cyber-safety* dalam penelitian ini juga menyangkut potensi risiko lainnya, iaitu: *Internet Addiction*.

Internet addiction atau kecanduan internet dalam penelitian ini mengacu pada perilaku ketergantungan yang berlebihan terkait penggunaan piranti digital dan atau media berbasis internet lainnya. Tentu juga meliputi kecanduan akan konten tertentu atau penggunaan gadget tertentu.

1.8 Metode Penelitian

1.8.1 Desain Penelitian

Penelitian ini dilakukan dengan menggunakan pandangan *contructivism*. Diambilnya pandangan tersebut didasari oleh kesepahaman peneliti dalam memandang permasalahan mengenai keselamatan siber pada anak. Sama seperti pandangan *constructivist* yang menganggap bahwa fenomena sosial adalah konstruksi sosial yang mana segala bentuk dan jenisnya dijiwai oleh nilai, norma dan asumsi (Halperin & Heath, 2012), demikian peneliti berasumsi bahwa keselamatan siber pada anak yang terjadi di Kota Semarang tidaklah ditemukan, melainkan terbentuk. Karena itu, kemudian penelitian ini dimaksudkan untuk menemukan sejauh mana keselamatan siber pada anak di Kota Semarang terjamin untuk keberlansungan anak-anak ke depannya.

Berangkat dari pandangan *contructivism* tersebut, kemudian peneliti akan melakukan penelitian kualitatif dengan mengambil pendekatan *case study* secara eksplanatori. Sehingga, penelitian ini dapat meneliti secara mendalam salah satu kasus dengan mendalam. Dalam konteks ini keselamatan siber pada anak merupakan kasus yang akan dikaji peneliti. Untuk memotret gambaran besar dari kasus tersebut, maka peneliti memecahnya kedalam beberapa isu: pornografi *online* anak, *cyber-bullying* anak dan kecanduan internet. Isu-isu tersebut kemudian dikaji dengan teknik analisis wacana sebelum kasus tentang keselamatan siber anak di Kota Semarang dapat dianalisis lebih lanjut.

1.8.2 Situs Penelitian

Penelitian ini di lakukan di Kota Semarang. Daerah ini dipilih karena mengingat merupakan salah satu kota besar di Indonesia. Terlebih, literasi

terkait keamanan anak di dunia maya di kota ini masih jarang ditemukan. Tetapi bukan berarti tidak ada masalah terkait keamanan digital, justru karena tidak terekspos, masyarakat jadi enggan merasa resah. Walaupun begitu, sebenarnya, baru pada akhir juni 2019, tedapat 20 anak yang mengalami gangguan jiwa karena kecanduan gadget (Utama, 2019).

1.8.3 Subjek Penelitian

Subjek dalam penelitian ini akan dibagi menjadi dua, meliputi pemerintah dan lembaga non pemerintah. Dari pemerintah, terdiri atas Dinas Kominfo Kota Semarang, Dinas Dinas Pemberdayaan Perempuan dan Perlindungan Anak (DP3A) Kota Semarang, Rumah Sakit Jiwa Daerah Dr. Amino Gondohutomo, Rumah Duta Revolusi Mental Kota Semarang.

Sedangkan lembaga non-pemerintah (NGO) meliputi: Yayasan Setara dan Pilar PKBI Jateng. Lalu, juga turut mewawancarai dua orang anak beserta orangtua dan wali mereka. Terkahir, mewawancarai seorang pemerhati anak yang juga Manager Klub Merby Kota Semarang yang tergolong kedalam sisi privat/swasta.

1.8.4 Jenis dan Sumber Data

Jenis data dalam penelitian ini berupa teks, kata-kata tertulis, foto dan sebagian berupa angka. Adapun sumber data yang digunakan untuk membantu penelitian berupa:

a. Data Primer

Untuk mendapatkan data primer, dalam penelitian ini dilakukan dengan cara wawancara. Wawancara merupakan proses tanya jawab yang ditujukan terhadap informan (Wahyuni, 2012). Tekni pengumpulan data ini kemudian terbagi lagi dalam beberapa jenis, seperti: wawancara tatap muka secara individu, wawancara telepon, wawancara online. Bentuknya pun terbagi lagi menjadi wawancara terstruktur, tidaka terstruktur dan semi-terstruktur. Penelitian ini menggunakan wawancara tatap muka dengan pertanyaan semi-terstruktur.

b. Data Sekunder

Untuk mengimbangi hasil kedua wawancara dan menggali lebih dalam data primer yang di dapat, maka penelitian ini diikuti oleh *literature research/literature review*. *Literature review* ini memili fungsi ganda, yaitu untuk membuat rumusan pertanyaan dan untuk menjadi dasar elaborasi argument (Halperin & Heath, 2012). Data yang didapat dari literasi ini kemudian juga digunakan sebagai validasi hasil wawancara.

1.8.5 Teknik Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam pelaksanaan penelitian ini adalah:

1. **Wawancara atau interview**, yang dilakukan dengan mewawancarai berbagai aktor yang terlibat sebagai narasumber dalam penelitian ini. Untuk memperkuat akurasi data temuan, dalam wawancara akan dilakukan dengan menggunakan triangulasi, yang berarti ada pertanyaan-pertanyaan yang bersifat mengonfirmasi

jawaban-jawaban dari narasumber sebelumnya. Adapun dalam mengurai hal tersebut, narasumber yang diwawancari meliputi: Krisna Thiyastika (pemerhati anak), Nopal (anak) & Rossi (wali anak), Sekar (anak) & Warsilah (ibu), Sri Mulyani (Dokter Klinis Kejiwaan RSJD Dr. Amino Gondohutomo).

Kemudian, peneliti juga mewawancari sektor-sektor primer yang terkait dengan kebijakan proteksi anak yang meliputi: Wulan & Aziz (Pilar PKBI), Eko Kurnia (Diskominfo Kota Semarang), Tegoeh Tri Adijanto (Kabid. Pemenuhan Hak Anak DP3A), Catur Karyanti (Kasi Pengasuhan, Pendidikan, Budaya DP3A), Bintang Al-Huda (Yayasan Setara), Putri Marlenny (RDRM).

2. ***Literature review*** yang digunakan untuk membantu dalam melakukan konseptualisasi, membandingkan dan generalisasi dari data-data yang telah dikumpulkan (Denzin, 2009). *Literature review* yang digunakan bersumber dari jurnal dan artikel dari penelitian yang sudah dilakukan. Dalam pembahasan, sumber-sumber ini digunakan untuk triangulasi hasil wawancara.

3. Dokumentasi, yaitu menggunakan bentuk-bentuk dokumen yang diperlukan untuk melengkapi temuan dalam penelitian ini. Hal ini berupakan temuan unggahan problematik yang dilakukan anak di dunia siber.

1.8.6 Pengolahan Data

Dalam penelitian ini, pengolahan data dilakukan dengan kegiatan- kegiatan sebagai berikut:

1. Recording, yaitu proses merekam wawancara. Selain merekam, dapat pula melakukan pencatatan *note.* Hal ini diperlukan untuk mengantisipasi hal-hal yang terlupakan saat melakukan wawancara. Pencatatan note diperlukan untuk mencatat hal-hal penting, termaksud hasil observasi jawaban non-verbal responden (Halperin & Heath, 2012).

2. Editing, yaitu mengolah kembali data yang ditemukan untuk mematangkan temuan, secara substansi maupun redaksional.

3. Presenting, yaitu suatu cara untuk merepresentasikan data ke dalam bentuk yang mudah untuk dimengerti.

1.6.7 Analisis dan Interpretasi Data

Analisis data adalah proses pengolahan data dari data primer ke dalam bentuk data yang lebih mudah dimengerti, dan diinterpretasikan. Adapun alur kegiatan dalam analisis ini adalah:

1. Transkrip data, menulis ulang hasil wawancara. Pada saat melakukan transkrip, peneliti juga akan menyeleksi data-data atau informasi yang dianggap penting untuk menunjang penelitian. Data-data yang di transkrip ini akan membantu proses coding (Denzin, 2009).

2. Coding, mengategorisasikan data-data temuan di lapangan ke dalam beberapa kategori berbeda yang didasarkan pada topik penelitian, hal ini dilakukan untuk membantu melakukan analisis terhadap hasil penelitian (Denzin, 2009).

3. Analisis, menganalisis semua data, dari sumber manapun untuk menemukan keterkaitan di antara data-data tersebut dan menyimpulkan hasil temuan (Denzin, 2009).