BAB I

PENDAHULUAN

1.1 Latar Belakang

Peran teknologi 5.0 telah membawa dampak besar bagi peradaban manusia untuk menjelajahi dunia melalui Internet. Pengguna teknologi sosial media perlu menjadi orang yang sadar secara teknis dan antusias karena perhatian orang terfokus pada pengembangan dunia teknologi atau siber yang sudah hidup berdampingan dengan manusia. Perkembangan dunia teknologi informasi telah mendukung berbagai kemajuan di berbagai bidang, seperti pendidikan, pekerjaan, kesehatan, sarana dan prasarana, yang dapat memudahkan aktivitas sehari-hari orang tersebut. Bahkan, revolusi industri 5.0 membuat perubahan dalam mentalitas manusia dalam kehidupan dan masyarakat. Pada era ini akan berkontribusi pada berbagai kegiatan sosial di berbagai bidang, terutama di bidang teknologi. Namun tidak hanya itu, konsekuensi yang dihasilkan mempengaruhi berbagai sektor, yaitu politik, ekonomi, sosial, serta hukum.

Untuk segala sesuatu yang menggunakan teknologi sebagai kebutuhan informasi, sebagai data pribadi untuk mengumpulkan data dari arsip publik, dan untuk kebutuhan lain seperti perbankan, tenaga kerja, bisnis, pendidikan dan fasilitas pemerintah seperti transportasi, yang tentunya menggunakan data pribadi untuk pencatatan sebagai data pengguna. Perkembangan teknologi informasi merupakan salah satu ilmu yang paling cepat berkembang dibandingkan dengan ilmu-ilmu lainnya. Tanpa disadari kita bisa merasakan efeknya selama ini, dengan berbagai fasilitas yang

dihadirkan bahkan dengan Internet bisa menjadi karya bagi sebagian orang. Seseorang bebas melakukan sesuatu yang mendukung pengetahuan teknologi, tentunya dalam hal ini pemerintah harus bisa mengatur lebih lanjut dan bisa masuk kerajaan agar pelanggaran yang ditimbulkan tidak terjadi.

Sebagai bentuk inovasi, teknologi informasi kini telah mampu mengumpulkan, menyimpan, membagikan dan menganalisis data yang sebelumnya tidak dapat dibayangkan, sehingga dikembangkan hak atas privasi untuk mengartikulasikan hak untuk melindungi data pribadi. Konsep perlindungan data mensyaratkan bahwa individu memiliki hak untuk menentukan apakah mereka akan membagikan atau berbagi data pribadi satu sama lain, serta hak untuk menentukan syarat apa yang harus dipenuhi.

Perlindungan data adalah kunci untuk masalah bisnis dan ekonomi dalam bisnis informasi di era modern. Praktik bisnis modern saat ini sering melibatkan manipulasi data, seperti segmentasi data pelanggan, termasuk penambangan dan pemilihan data, pembuatan profil pelanggan, konsolidasi pemrosesan data global, dan proses bisnis lainnya. Dari kemajuan teknologi informasi, muncul tindakan melawan hukum. Dalam kasus kebocoran data pribadi, Indonesia tidak memiliki perlindungan terkait data privasi atau undang-undang yang mengatur perlindungan data pribadi, sehingga rentan terhadap kebocoran data. Rawan terjadi penyalahgunaan atas data pribadi tersebut yang seharusnya menjadi hak privasi setiap warga negara seperti dalam kasus pemalsuan data diri dalam Putusan Pengadilan Nomor 541/Pid.Sus/2022/PN Mdn. Dalam kasus tersebut, terdapat 4 Terdakwa

yang diadili atas dakwaan mengenai penyalahgunaan identitas Data Pribadi dalam situs bantuan Prakerja yang difungsikan sebagai warga negara yang kehilangan pekerjaan akibat dampak Pandemi Covid – 19 selama 2 tahun terakhir untuk mendapatkan pekerjaan kembali melalui pelatihan yang diselenggarakan oleh Pemerintah sebagai upaya untuk meminimalisir jumlah pengangguran dan PHK Massal serta memberikan dana kepada mereka yang kehilangan pekerjaannya sebagai bentuk bantuan Pemerintah atas kebutuhan pokok yang harus tetap dipenuhi. Diketahui sebanyak 1.100 akun (seribu seratus) akun / peserta terdaftar dengan menggunakan identitas hasil kebocoran data NIK yang telah diperjual – belikan dan dipalsukan sebagai data diri milik orang lain untuk mendapat dana dari pemerintah. Perbuatan melawan hukum *cyber* sangat tidak mudah diatasi dengan mengandalkan hukum positif konvensional karena berbicara mengenai kejahatan, tidak dapat dilepaskan dari lima faktor yang saling terkait, yaitu pelaku kejahatan, modus kejahatan, korban kejahatan, reaksi sosial atas kejahatan dan hukum.[1] Hukum menjadi instrumen penting dalam pencegahan dan penanggulangan kejahatan, di samping instrumen – instrumen lain yang tidak kalah penting. Akan tetapi, untuk membuat suatu ketentuan hukum terhadap bidang hukum yang berubah sangat cepat, seperti teknologi informasi bukanlah suatu perkara yang mudah. Disinilah sering kali hukum (peraturan) tampak cepat menjadi usang manakala mengatur bidang yang mengalami perubahan yang cepat, sehingga situasinya seperti terjadi kekosongan hukum (*Vaccum Rechts*).

[1] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta: Rajagrafindo Persada, 2013), hlm. 4.

Kejahatan di dunia *cyber* sangat sulit untuk dapat menjerat pelaku. Hal ini dibuktikan dari banyaknya kasus *cybercrime* yang tak dapat dituntaskan oleh sistem peradilan Indonesia. Persoalannya terdapat pada sulitnya mencari pasal – pasal yang dapat dipakai sebagai landasan tuntutan di Pengadilan kepada pelaku penyalahgunaan teknologi (*Cybercrime*) berdasarkan Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik sebagai terobosan untuk dapat menjadi landasan dan perluasan asas – asas beserta sanksi pidananya yang saat ini telah mengalami amandemen menjadi Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Berdasarkan latar belakang tersebut, penulis tertarik mengambil judul Proposal Skripsi yaitu **"KAJIAN YURIDIS TINDAK PIDANA PEMALSUAN IDENTITAS DATA DIRI DALAM SITUS BANTUAN KARTU PRAKERJA"**

1.2 Rumusan Masalah

1. Apa yang menjadi alasan terjadinya transaksi jual beli data pribadi dalam situs bantuan kartu Prakerja?
2. Bagaimana perlindungan bagi pemilik identitas data diri yang dipalsukan dalam situs bantuan kartu Prakerja?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk :

1. Mengetahui alasan mengapa terjadinya kasus jual beli data pribadi pada situs bantuan kartu Prakerja.

2 Mengetahui bentuk perlindungan bagi pemilik identitas data diri yang dipalsukan dalam situs bantuan kartu Prakerja menurut hukum positif di Indonesia

1.4 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut :

1. Secara Teoritis

   Secara teoritis, penelitian ini dapat berguna bagi perkembangan Ilmu Hukum Pidana khususnya dalam penerapan penggunaan teknologi informasi (*Cyber Crime*).

2. Secara Praktis

   Secara praktis, penelitian ini diharapkan dapat memberikan informasi dan masukan :

   1. Diharapkan dapat digunakan sebagai sumbangan pemikiran dan atau setidaknya memberikan pengetahuan terkait pengaturan tentang pemalsuan identitas data diri yang disalahgunakan untuk kepentingan pribadi.
   2. Dengan adanya penelitian ini dapat membantu memberikan informasi serta pemahaman dan terkait pengaturan tentang penyalahgunaan data diri di bidang teknologi menurut hukum positif di Indonesia.

1.5 Tinjauan Pustaka

1.5.1 Tinjauan Umum Tentang Tindak Pidana Pemalsuan Identitas Data Diri dalam Sistem Teknologi Informasi

1.5.1.1 Pengertian Informasi Pribadi dan Data Pribadi

Informasi pribadi mengandung dua pengertian yaitu informasi dan pribadi. Informasi berarti keterangan atau penerangan dari data yang telah diproses ke dalam suatu bentuk yang mempunyai arti bagi si penerima dan nilainya nyata sehingga dapat dipakai sebagai dasar untuk mengambil keputusan. Data adalah fakta atau bagian dari fakta yang mengandung arti yang dihubungkan dengan simbol-simbol, gambar, kata-kata, angka, huruf, atau simbol-simbol yang menunjukkan objek, kondisi atau situasi-situasi lain.[2]

Istilah perlindungan data pertama digunakan di Jerman dan Swedia pada tahun 1970-an yang mengatur perlindungan data pribadi melalui undang-undang. Alasan dibuatnya undang-undang perlindungan data karena pada waktu itu mulai dipergunakan komputer sebagai alat untuk menyimpan data penduduk terutama untuk keperluan sensus penduduk. Ternyata dalam praktik, telah terjadi banyak pelanggaran yang dilakukan baik oleh pemerintah mauapun pihak swasta. Adanya penelitian yang diadakan oleh *National Research Council,* menyatakan bahwa pengertian *personal information* adalah semua data yang berkaitan dengan individu tertentu seperti: tanggal

[2] DR. Shinta Dewi, S.H., LL.M., *Cyber Law 1 : Perlindungan Privasi atas Informasi Pribadi Dalam E-Commerce Menurut Hukum Internasional*, (Bandung: Widya Padjajaran, 2009). Hlm. 36

kelahiran, jenis kelamin, alamat, pendidikan, hobi, dan apabila di *profiling*, maka akan menghasilkan data khusus tentang seseorang.[3] Menurut Wacks[4], pengertian mengenai informasi pribadi yaitu :

> *Personal information consist of those facts, communications, or opinions which relate to the individual and which it would be reasonable to expect him to regard as intimate or sensitive and therefore to want to withold or at least to restrict their collection, use, or circulation.*

Setiap negara memiliki penyebutan yang berbeda mengenai informasi pribadi. Amerika Serikat, Kanada, dan Australia menggunakan istilah informasi pribadi, sedangkan negara-negara di Uni Eropa dan Indonesia menggunakan data pribadi. Definisi data pribadi dapat ditemukan dalam peraturan perundang-undangan antara lain:

a) Pasal 1 nomor 1 dan 2 Peraturan Menteri Komunikasi dan Informatika No. 20 tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik menyebutkan bahwa data pribadi dimaksudkan sebagai identitas seseorang yang terang dan jelas yang merupakan penetapan bukti diri terhadapnya yang dipelihara, dijaga kebenarannya dan ditempatkan dengan aman kerahasiannya. Sementara Pasal 2 angka 1 mengatur terhadap perolehan, pengumpulan, pengolahan, penganalisisan, penyimpanan, penampilan, pengumuman, pengiriman, penyebarluasan dan pemusnahan data pribadi merupakan perlindungan data pribadi

[3] Ibid, hlm. 38
[4] Ibid, hlm. 36

dalam sistem elektronik yang menghormati data pribadi sebagai privasi.

b) Pasal 1 nomor 27 Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, mendefinisikan data pribadi sebagai data perseorangan tertentu yang disimpan dan dijaga kebenaran serta dilindungi kerahasiannya.

Privasi adalah suatu konsep yang meliputi hak untuk mempunyai pemikiran sendiri, hak untuk mempunyai kewenangan untuk mengontrol diri sendiri, hak untuk dapat menyendiri dan kewenangan untuk mengontrol informasi sendiri termasuk di dalamnya adlah kebebasan untuk tidak diawasi, perlindungan terhadap reputasi seseorang dan perlindungan dari penggeledahan dan initerogasi.[5] Perlindungan privasi atas informasi pribadi berkembang disebabkan oleh pengguna internet dan banyaknya transaksi malalui *e-commerce* mengakibatkan banyaknya informasi pribadi yang dapat diproses, diprofilkan, dan kemudian disebarkan kapada pihak lain. Kegiatan-kegiatan dalam *e-commerce* yang telah melanggar privasi informasi seseorang adalah melalui cara yang dikenal dengan :[6]

1. Teknik pemrosesan data atau *data processing technologies*. Contohnya yaitu penyusunan pusat data dengan mempergunakan komputer (*computer data base*) biasanya dilakukan oleh badan pemerintah dalam melakukan tugasnya sehari-hari sehingga dapat mengumpulkan infromasi penduduk, terutama dengan konsep *e-government* sehingga informasi penduduk dapat dikoleksi kemudian di kirimkan antara lembaga pemerintah. Bahkan pihak swasta juga sekarang telah mempunyai pusat dan biasanya mengenai informasi keungan, alamat, latar belakang, pendidikan.

[5] Ibid, hlm. 46
[6] Ibid, hlm. 35

2. Pencarian Data atau *data mining* melalui transaksi internet maka informasi pribadi seseorang dapat dikumpulkan oleh pihak industri.
3. *Cookies* yaitu serangkaian teks yang dikirimkan oleh *server* ke penjelajah web untuk mengetahui situs-situs mana yang telah dikunjungi oleh seseorang sehingga dapat diketahui informasi spesifik seseorang seperti preferensi situs-situs yang dikunjungi.
4. *Web Bug* adalah suatu alat perekam yang tersembunyi yang dapat merekam pesan-pesan *e-mail.*
5. *Carnivore* suatu alat yang dikembangkan oleh FBI untuk dapat memonitor *email* yang dikirim melalui atau menuju perusahaan penyedia jasa internet (*internet service provider).*

1.5.1.2 Tindak Pidana Pemalsuan Identitas

Marak "Kartu Tanda Penduduk (KTP) sebagai identitas diri sangat penting bagi pemerintah untuk pengurusan administrasi kependudukan dan pengolahan data penduduk. Pada saat masih sering banyak kasus pemalsuan KTP yang dapat berakibat menjadi suatu tindak criminal. NIK (Nomor Induk Kependudukan) sebagai Identitas penting dapat berubah-ubah karena setiap daerah berbeda-beda. Proses pembuatan KTP dilakukan secara manual membutuhkan waktu proses yang lama dan terkadang tidak efektif, proses yang seperti ini kadang membuat masyarakat enggan untuk melakukan pengurusan KTP. Identitas yang seharusnya menjadi salah satu tanda pengenal jati diri maupun status yang benar dari seseorang dipalsukan. Kejahatan pemalsuan Identitas mengandung sistem ketidak benaran atau palsu atas suatu hal (objek) yang sesuatunya itu nampak dari luar seolah-olah benar adanya, padahal sesungguhnya bertentangan dengan yang sebenarnya. Perbuatan pemalsuan Identitas merupakan suatu jenis pelanggaran terhadap

dua" normadasar.[7]

1. Kebenaran" ("kepercayaan) yang pelanggaranya dapat tergolong dalam kelompok kejahatan penipuan.

2. Ketertiban masyarakat, yang pelanggaranya tergolong dalam kelompok kejahatan terhadap Negara".

Perbuatan pemalsuan merupakan suatu jenis pelanggaran terhadap kebenaran dan keterpercayaan, dengan tujuan memperoleh keuntungan bagi diri sendiri atau orang lain. Suatu pergaulan hidup yang teratur di dalam masyarakat yang maju teratur tidak dapat berlangsung tanpa adanya jaminan kebenaran atas beberapa bukti surat dan dokumen-dokumen lainnya. Oleh karenanya perbuatan pemalsuan dapat merupakan ancaman bagi kelangsungan hidup dari masyarakat tersebut. [8]

Pemalsuan identitas merupakan bentuk kejahatan yang dapat menimbulkan kerugian bagi pihak lain, berupa pemalsuan identitas yang dirubah agar seolah- olah benar adanya padahal tidak sesuai dengan kenyataannya.

1.5.1.3 Tindak Pidana Pemalsuan Identitas Menurut KUHP

Dalam lingkup Perbankan dimana segala sesuatu baik akses maupun meng-*input* data dibutuhkan identitas diri guna kepastian bahwa seseorang tercatat sebagai warga negara Indonesia dan dianggap telah cakap untuk menggunakan sarana Perbankan guna

[7] Evi Purnamawati, Warmiyana Zairi Absi dan Rusniati. "Pemalsuan Identitas Oleh Penjual Kartu (SIM) *Subscriber Identity*", *Jurnal Unpal*, Volume 20, Nomor 2, Mei 2022. Hlm. 224

[8] *Ibid,* hlm. 227.

kepentingan pribadi. Tentunya saat ini teknologi sebagai jembatan untuk menghubungkan segala data maupun dokumen untuk keperluan Perbankan agar terkoordinasi dengan baik.

Sudah menjadi tanggung jawab pribadi mengenai kelengkapan identitas data diri sebagai bentuk privasi agar tidak disalahgunakan seperti halnya pemalsuan identitas data diri. Dalam dunia perbankan, hal tersebut sangat rawan terjadinya penyalahgunaan. Hal tersebut dikarenakan identitas adalah suatu hal yang patut dijaga kerahasiaannya karena data pribadi tersebut merupakan privasi yang dilindungi oleh negara.

Pemalsuan identitas data diri menurut Pasal 378 KUHP menyebutkan barangsiapa dengan sengaja memasukkan nama atau identitas pribadi, melakukan tipu muslihat, kebohongan untuk mendapatkan keuntungan secara pribadi maka disebut sebagai tindakan penipuan dengan hukuman maksimal 4 tahun penjara.

1.5.1.4 Pemalsuan Identitas dalam Administrasi Kependudukan

Dalam perspektif perundang-undangan Indonesia, Administrasi Kependudukan diatur di dalam Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan (selanjutnya disebut Undang-Undang Administrasi Kependudukan).[9]

[9] Arie Julian Saputra, "Pertanggung Jawaban Pidana Pelaku Pemalsuan Dokumen Kependudukan Dalam Undang – Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan", *Jurnal Legalitas*, Volume 1, Nomor 5, Desember 2011. hlm. 204

Adapun bentuk-bentuk dari dokumen kependudukan tersebut, pada intinya meliputi antara lain Nomor Induk Kependudukan (NIK), Kartu Keluarga (KK), Kartu Tanda Penduduk Elektronik (KTP-el), Akta/Surat Nikah/Cerai, Akta Kelahiran/Kematian, Akta Pengesahan Anak, Pengangkatan Anak, Perubahan Nama dan Perubahan Status Kewarganegaraan. Sekilas pemalsuan dokumen kependudukan tampak sederhana, dan sudah lazim terjadi. Namun demikian, meskipun kelihatannya sederhana, pemalsuan dokumen kependudukan dapat menimbulkan dampak yang serius, yakni munculnya berbagai tindak pidana di tengah masyarakat.

Selain itu, perbuatan pemalsuan atau penyalahgunaan dokumen kependudukan, tersebut juga dapat dikenakan ancaman pidana sesuai ketentuan Pasal 93 Undang-Undang Administrasi Kependudukan yang menyatakan:

"Setiap Penduduk yang dengan sengaja memalsukan surat dan/atau dokumen kepada Instansi Pelaksana dalam melaporkan Peristiwa Kependudukan dan Peristiwa Penting dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 50 juta."

Perkembangan teknologi informasi saat ini berpengaruh yang sangat besar bagi kehidupan manusia yaitu mampu melaksanakan pengumpulan dan penyimpanan berbagai hal salah satunya data pribadi. Sejumlah instrumen internasional telah mengatur prinsip-prinsip perlindungan data dan banyak aturan-aturan nasional telah

memasukannya sebagai bagian dari hukum nasional. *The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No.108), 1981; the Organization for Economic Cooperation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)* adalah beberapa contoh instrumen internasional yang mengatur perlindungan data.[10] Konsep mengenai perlindungan data pribadi memiliki dasar bahwa setiap individu memiliki hak untuk menentukan mengenai apakah dirinya akan bergabung dan membagikan data pribadinya, Hukum hadir sebagai media perlindungan data pribadi mencakup langkah-langkah perlindungan terhadap keamanan data pribadi serta mengenai penggunaan data pribadi seseorang.[11] Data pribadi menurut Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data pribadi Dalam Sistem Elektronik[12] dalam Pasal 1 angka (1) adalah data perseorangan tertentu yang disimpan, dirawat dan dijaga kebenaran serta kerahasiaannya ; Pasal 1 angka (2), Data Perseorangan Tertentu adalah setiap keterangan yang benar dan nyata yang melekat dan

[10] Sinta Dewi, "Konsep Perlindungan Hukum Atas Privasi dan Data Pribadi Dikaitkan dengan penggunaan Cloud Computing di Indonesia", *Jurnal Yustisia*, Volume 5, Nomor 1, Januari-April 2016, hlm. 26

[11] *Ibid*, hlm. 25.

[12] Indonesia, Peraturan Menteri Komunikasi dan Informasi Tahun 2015 Tentang Perlindungan Data Pribadi Dalam SIstem Elektronik

dapat diidentifikasi baik langsung maupun tidak langsung pada masing-masing individu yang pemanfaatannya sesuai ketentuan peraturan perundang-undangan.

Data pribadi dapat berubah menjadi big data setelah organisasi berhasil mengumpulkan data dalam jumlah besar karena setiap dari kita akan menyumbangkan jumlah data yang cukup besar saat setiap kali melakukan kegiatan pada perangkat digital yang kita gunakan.[13] Big data adalah volume data dalam jumlah besar yang ada atau tersedia dalam lalu lintas informasi seperti email, pembelian atau pembelanjaan online, dan setiap klik pada situs web akan disimpan pada setiap server yang telah dibuka. Pengendalian informasi pribadi yang kita miliki harus lebih kuat dan ketat terhadap privasi yang kita miliki, oleh karena itu rezim perlindungan data mengatur pengumpulan, penggunaan dan pengungkapan data pribadi sangat dibutuhkan guna mengatasi dan menjaga kepercayaan masyarakat terhadap organisasi dan penyelenggara yang berhubungan dengan data tersebut.

1.5.1.5 Program Kartu Prakerja

Program Kartu Prakerja adalah program pengembangan kompetensi kerja yang ditujukan untuk pencari kerja, pekerja/buruh yang terkena pemutusan hubungan kerja, dan/atau pekerja/buruh yang membutuhkan peningkatan kompetensi.[14] Program Kartu

[13] Setyawati Fitri Anggraeni, "Polemik Pengaturan Kepemilikan Data Pribadi : Urgensi Untuk Harmonisasi Dan Reformasi Hukum Di Indonesia", *Jurnal Hukum & Pembangunan*, Vol. 48, No. 4, Oktober 2018. Hlm.

[14]Web Kementrian Bidang Koordinator Perekonomian Republik Indonesia, *"Tentang*

Prakerja bertujuan untuk mengembangkan kompetensi angkatan kerja, meningkatkan produktivitas dan daya saing angkatan kerja, serta mengembangkan kewirausahaan.

Pendaftaran Kartu Prakerja di tujukan bagi pencari kerja, pekerja/buruh yang terkena PHK, atau pekerja/buruh yang membutuhkan peningkatan kompetensi kerja, seperti pekerja/buruh yang dirumahkan dan pekerja bukan penerima upah, termasuk pelaku usaha mikro dan kecil. Untuk itu, harus memenuhi persyaratan sebagai warga negara Indonesia berusia paling rendah 18 (delapan belas) tahun dan tidak sedang mengikuti pendidikan formal. Untuk merespon dampak dari pandemi COVID-19, Program Kartu Prakerja untuk sementara waktu akan diprioritaskan bagi pekerja/buruh yang dirumahkan maupun pelaku usaha mikro dan kecil yang terdampak penghidupannya. Difabel juga dianjurkan untuk mendaftar dan mengikuti Program Kartu Prakerja. Berikut adalah daftar pekerjaan yang tidak bisa mengikuti program Prakerja, yaitu :

a. Pejabat Negara
b. Pimpinan dan Anggota Dewan Perwakilan Rakyat Daerah
c. Aparatur Sipil Negara
d. Prajurit Tentara Nasional Indonesia
e. Anggota Kepolisian Negara Republik Indonesia
f. Kepala Desa dan perangkat desa

Kartu Prakerja", 2022, https://www.prakerja.go.id/tanya-jawab/tentang-kartu-prakerja (Diakses pada 15 Agustus 2022, pukul 16.52 WIB)

g. Direksi, Komisaris, dan Dewan Pengawas pada badan usaha milik negara atau badan usaha milik daerah

Dalam 1 (satu) Kartu Keluarga hanya diperbolehkan maksimal 2 (dua) NIK yang menjadi Penerima Kartu Prakerja. Hanya warga negara Indonesia yang berumur minimal 18 tahun dan maksimal 64 tahun yang dapat menjadi Penerima Kartu Prakerja.

Solusi yang ditawarkan pada program Kartu Prakerja diantaranya membantu meringankan biaya pelatihan yang ditanggung pekerja dan perusahaan. Mendorong kebekerjaan dengan mengurangi *mismatch*, mengurangi biaya untuk mencari informasi mengenai pelatihan, menjadi komplementer dari pendidikan formal, dan membantu daya beli masyarakat yang terdampak mata pencahariannya akibat COVID-19.

Manajemen Pelaksana sebagai unit yang melaksanakan Program Kartu Prakerja dan berada di bawah Kementerian Koordinator Bidang Perekonomian Republik Indonesia yang akan melaksanakan operasional Kartu Prakerja. Komite Cipta Kerja dibentuk melalui Peraturan Presiden Nomor 36 Tahun 2020 tentang Pengembangan Kompetensi Kerja melalui Program Kartu Prakerja sebagaimana telah diubah dengan Peraturan Presiden Nomor 76 Tahun 2020. Komite bertugas merumuskan dan menyusun kebijakan Program Kartu Prakerja serta melakukan pengendalian dan evaluasi pelaksanaan Program Kartu Prakerja.[15] Semua kebijakan Kartu

[15] *Ibid*.

Prakerja dirumuskan oleh Komite Cipta Kerja yang diketuai oleh Menteri Koordinator Bidang Perekonomian dan Kepala Staf Kepresiden sebagai Wakil Ketua, terdiri dari 12 (dua belas) menteri dan kepala lembaga sebagai anggota dan Sekretaris Kementerian Koordinator Bidang Perekonomian sebagai Sekretaris Komite.

1.5.2 Tinjauan Umum Tentang Kejahatan Siber (*Cyber Crime*)

1.5.2.1 Pengertian *Cyber Crime*

Pada masa awalnya, *Cyber Crime* didefinikasn sebagai kejahatan komputer. *The British Law Commision* mengartikan "*computer fraud"* sebagai manipulasi komputer dengan cara apapun yang dilakuan dengan itikad buruk untuk memperoleh uang, barang atau keuntungan lainnya atau dimaksudkan untuk menimbulkan kerugian kepada pihak lain.[16] Pada dasarnya *cyber crime* merupakan kegiatan yang memanfaatkan komputer sebagai sarana atau media yang didukung oleh system telekomunikasi, baik menggunakan telepon atau *wireless system* yang menggunakan antena khusus seperti nirkabel. Hal inilah yang disebut "telematika" yaitu konvergensi antar teknologi telekomuniksi, media, dan informatika yang semula masing-masing berkembang secara terpisah.[17]

Sistem teknologi informasi berupa internet telah dapat

[16] Budi Suhariyanto, *Tindak Pidana Teknologi Informasi (Cybercrime)*, (Jakarta: Rajagrafindo Persada, 2013), hlm. 9-10

[17] Rini Retno Winarni, 2016, "Efektivitas Penerapan Undang – Undang ITE Dalam Tindak Pidana *Cyber Crime*". *Jurnal Hukum dan Dinamika Masyarakat*, Vol. 14 No. 1. Hlm 18

mengeser paradigma para ahli hukum terhadap definisi kejahatan omputer sebagaimana ditegaskan sebelumnya, bahwa pada awalnya para ahli hukum terfokus pada alat/ perangkat keras yaitu komputer. Namun dengan adanya perkembangan teknologi informasi berupa jaringan internet, maka fokus dari identifikasi terhadap definisi *cybercrime* lebih diperluas lagi yaitu seluas aktivitas yang dapat dilakukan di dunia *cyber/*maya melalui sistem informasi yang digunakan.[18] Adanya Kejahatan Siber (*Cyber Crime*) telah menjadi ancaman stabilitas, sehingga pemerintah sulit mengimbangi teknik kejahatan yang dilakukan dengan teknologi komputer, khususnya jaringan internet dan intranet (Ketaren, 2016:35).[19] *Council of Europe Conventiom on Cyber Crime (COECCC)*, telah diselenggarakan pada tanggal 23 November 2001 di Kota Budapest, Hongaria. Konvensi ini telah menyepakati bahwa *Convention on Cyber Crime* dimasukkan dalam *Europe Treaty Series* dengan nomor 185.[20] Konvensi ini akan berlaku efektif setelah diratifikasi oleh minimal 5 (lima) negara dan tiga negara anggota *Council of Europe*. Substansi konvensi ini mencakup area yang cukup luas, bahkan mengandung kebijakan kriminal yang bertujuan untuk melindungi masyarakat dari *cyber crime*, baik melalui undang-undang maupun kerja sama internasional. Konvensi ini telah disepakati oleh masyarakat Uni Eropa sebagai

[18] Budi Suhariyanto, *Op. Cit.*, hlm. 11

[19]Hardiyanto Djanggih, Nurul Qamar, "Penerapan Teori - Teori Kriminologi Dalam Penanggulangan Kejahatan Siber (*Cyber Crime*)", *Jurnal Pandecta*, Vol. 13, No. 1, Juni 2018. Hlm. 12

[20] Resa Raditio, S.H., M.H., *Aspek Hukum Transaksi Elektronik*. (Yogyakarta: Graha Ilmu, 2014). Hlm. 33

konvensi yang terbuka untuk diakses oleh negara manapun di dunia. Hal ini dimaksudkan untuk dijadikan norma dan instrumen hukum internasional dalam mengatasi kejahatan siber, tanpa mengurangi kesempatan setiap individu untuk tetap dapat mengembangkan kreativitasnya dalam pengembangan teknologi informasi.

1.5.2.2 Cyber Crime Menurut KUHP

Kitab Undang – Undang Hukum Pidana (KUHP) telah mengatur hubungan – hubungan hukum tentang kejahatan yang berkaitan dengan dengan komputer (*computer crime*) yang kemudian berkembang menjadi *Cybercrime*. Keterdesakan kebutuhan nasional ini bisa dilihat dari adanya fakta bahwa aturan – aturan yang konvensional tidak dapat diandalkan dalam upaya penanggulangan kejahatan *cybercrime*, baik secara materiil (KUHP) maupun formal (KUHAP). Sebagaimana diketahui bahwa keberadaan KUHP dan KUHAP sebagai induk dari aturan hukum pidana dan acara pidana masih belum mampu menanggulangi kejahatan di dunia *cyber* yang berkaitan dengan tindak pidana yang baru (berdimensi dunia maya).

Ketentuan yang terdapat dalam KUHP mengenai *cybercrime* masih bersifat global. Jika ditinjau dari perspektif penafsiran hukum tentunya hal yang diatur secara global dalam KUHP dapat dilakukan penyesuaian secara praktis sebelum terakomodasi dalam undang – undang khusus yang mengaturnya secara terperinci.

1.5.2.3 *Cyber Crime* Menurut Undang – Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Unsur objektif dalam hal perumusan delik *cybercrime* mengalami beberapa terobosan dari sifat – sifat umum dari KUHP. Hal ini disebabkan kegiatan *cyber* meskipun bersifat virtual tetapi dikategorikan sebagai tindakan dan perbuatan hukum yang nyata. Ketentuan Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik tentunya merupakan bagian dari kerja normatif untuk melindungi bangsa Indonesia.

Sebenarnya, Undang-Undang Nomor 11 Tahun 2008 sebagai amandemen dengan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008) adalah undang-undang administratif. Namun, legislator memasukkan beberapa ketentuan tentang tindak pidana. Pada dasarnya *cyber crime* meliputi semua tiindak pidana yang berkenaan dengan sistem informasi, serta sistem komunikasi yang merupakan sarana untuk penyampaian/pertukaran informasi kepada pihak lainnya.[21]

Undang- Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik terdiri dari 13 bab dan 54 pasal yang merupakan peraturan hukum baru untuk mengatur kegiatan *cyber*

[21] Didik M. Arief Mansur dan Elistaris Ghultom, *Cyber Law-Aspek Hukum Teknologi Informasi*, (Bandung: Refika Aditama, 2005), hlm. 10

space di Indoensia. Beberapa aspek – aspek penting yang diatur dalam Undang - Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 sebagai berikut :[22]

1. Aspek Yurisdiksi
   Aspek ini digunakan pendekatan prinsip perluasan yurisdiksi (*Extra Territorial Yurisdiction*) dikarenakan transaksi elektronik memiliki karakteristik lintas teritorial dan tidak dapat menggunakan pendekatan hukum konvensional.
2. Aspek Pembuktian Elektronik
   Alat bukti elektronik merupakan alat bukti dan memiliki akibat hukum yang sah di muka pengadilan.
3. Aspek Informasi dan Perlindungan Konsumen
   Pelaku usaha yang menawarkan produk melalui media elektronik wajib menyediakan informasi yang lengkap dan benar, berkaitan dengan syarat – syarat kontrak, produsen dan produk yang ditawarkan.
4. Aspek tanda tangan elektronik
   Aspek tanda tangan elektronik memiliki kekutana hukum dan akibat hukum yang sah (sejajar dengan tanda tangan manual) selama memenuhi persyaratan sebagaimana ditetapkan dalam UNDANG - UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG - UNDANG NOMOR 11 TAHUN 2008.
5. Aspek pengamanan terhadap tanda tangan elektronik
   Setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya.
6. Aspek penyelenggara sertifikasi elektronik
   Setiap orang berhak menggunakan jasa penyelenggara sertifikasi elektronik untuk tanda tangan elektronik yang dibuat.
7. Aspek penyelenggara sertifikat elektronik, informasi dan transaksi elektronik
   Aspek penyelenggara sertifikat elektronik, informasi dan transaksi elektronik secara andal, aman, dan beroperasi sebagaimana mestinya serta penyelenggara sistem elektronik bertanggung jawab terhadap penyelenggaraan atau keamanan sistem elektronik yang diselenggarakannya.
8. Aspek tanda tangan digital (*Digital Signature*)
   Penggunaan tanda tangan digital dapat berubah sesuai dengan isi dokumen dan memiliki sifat seperti tanda tangan

[22] Dr. Danrivanto Budhijanto, *REVOLUSI CYBERLAW INDONESIA Pembaruan dan Revisi UNDANG - UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG - UNDANG NOMOR 11 TAHUN 2008 2016*, (Bandung: Refika Aditama, 2017), hlm. 5

konvensional sepanjang dapat dijamin kendalanya secara teknis.

9. Aspek transaksi elektronik

   Kegiatan transaksi elektronik dapat dilakukan baik dalam lingkup publik maupun privat dan transaksi elektronik yang dituangkan dalam kontrak elektronik mengikat para pihak serta para pihak memiliki kewenangan untuk memilih hukum yang berlaku bagi transaksi elektronik internasional yang dibuatnya.

10. Aspek nama domain

    Aspek nama domain yang digunakan sebagai Hak Kekayaan Intelektual (HKI) oleh seseorang, dimana orang yang dimaksud berhak memiliki nama domain berdasarkan prinsip *first come first serve* dan informasi elektronik yang disusunmenjadi karya intelektual, desain situs internet, dannkaarya-karya intelektual yang ada di dalamnya, dilindungi sebagai Hak Kekayaan Intelektual berdasarkan perundang-undangan yang berlaku.

11. Aspek perlindungan privasi

    Penggunaan setiap informasi melalui media elektronik yang menyangkut data tentang pribadi seseorang harus dilakukan atas persetujuan dari orang yang bersangkutan, kecuali ditentukan lain oleh peraturan perundang-undangan.

12. Aspek peran pemerintah dan masyarakat

    Pemerintah memfasilitasi pemanfaatan informasi dan transaksi elektronik dengan memperhatikan ketentuan peraturan perundang-undangan yang berlaku.

13. Aspek perlindungan kepentingan umum

    Pemerintah berwenang melindungi kepentingan umum dari segala jenis gangguan sebagai akibat penyalahgunaan informasi dan transaksi elektronik yang mengganggu ketertiban umum dan kepentingan nasional serta pemerintah menetapkan instansitertentu harus memiliki *back up e-data* dan *on-line*.

14. Aspek perbuatan-perbuatan yang dilarang sebagai berikut:
    a. Menyebarluaskan informasi elektronik yang bermuatan pornografi, perjudian, tindak kekerasan, penipuan;
    b. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperolah, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik;
    c. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperolah, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik milik pemerintah yang karena statusnya harus dirahasiakan atau dilindungi;

d. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik dengan cara apapun tanpa hak, dengan maksud untuk memperoleh, mengubah, merusak, atau menghilangkan informasi dalam komputer atau sistem elektronik menyangkut pertahanan nasional atau hubungan internasional yang dapat menyebabkan gangguan atau bahaya terhadap negara dan atau hubungan dengan subyek hukum internasional;
e. Melakukan tindakan yang secara tanpa hak yang menyebabkan transmisi dari program, informasi, kode atau perintah, komputer dan/atau sistem elektronik yang dilindungi negara menjadi rusak;
f. Menggunakan dan/atau mengakses komputer dan/atau sistem elektronik secara tanpa hak atau melampaui wewenangnya, baik dari dalam maupun dari luar negeri untuk memperoleh informasi dari komputer dan/atau sistem elektronik yang dilindungi oleh negara.

1.5.2.4 Macam – Macam Bentuk Tindak Pidana *Cyber Crime*

Terdapat banyak perbedaan di antara para ahli dalam mengklasifikasikan kejahatan *Cyber Crime*. Untuk memudahkan klasifikasi kejahatan *Cyber Crime*, dapat di simpulkan.[23]

1. Kejahatan-kejahatan yang menyangkut data atau informasi komputer.
2. Kejahatan-kejahatan yang menyangkut program atau software komputer.
3. Pemakaian fasilitas komputer tanpa wewenang untuk kepentingan-kepentingan yang tidak sesuai dengan tujuan pengelolaan atau operasinya.
4. Tindakan yang mengganggu operasi komputer.
5. Tindakan merusak peralatan komputer atau peralatan yang berhubungan dengan komputer atau sarana penunjangnya.

Munculnya berbagai kejahatan di dunia maya juga harus diibangi oleh penegakan hukum yang sedimikian rupa (usaha yang rasional) agar dimungkinkan pelaku-pelakunya dapat diproses secara hukum. Untuk memberikan pemahaman kepada kita semua (masyarakat), terutama mengenai kejahatan-kejahatan yang

[23] Abdul Wahid dan M. Labib, *Kejahatan Mayantara (Cyber Crime)*, (Bandung: Refika Aditama, 2005), hlm. 76

mungkin terjadi di dalam dunia maya, maka dalam kesempatan ini dapat penulis kemukakan sebagai berikut :[24]

1. *Carding* adalah suatu bentuk penyalahgunaan di dunia maya (*cybercrime*) dengan cara berbelanja menggunakan nomor dan identitas kartu kredit orang lain, yang diperoleh secara illegal (melawan hak), biasanya dengan mencuri data-data dari internet;
2. *Hacking* adalah kegiatan menerobos program komputer milik orang/pihak lain, dengan maksud-maksud tertentu secara melawan hak. Sedangkan Hacker sendiri adalah orang/pelaku yang gemar ngoprek komputer, memiliki keahlian membuat dan membaca program tertentu serta terobsesi mengamati ke amanannya. Hal ini dapat penulis contohkan ada akun media sosial (*facebook*) dari teman kita atau akun kita sendiri yang pernah dikuasai secara melawan hak oleh orang-orang yang tidak bertanggung jawab;
3. *Cracking* adalah suatu kegiatan hacking untuk tujuan jahat, sedangkan "*cracker*" adalah "hacker" bertopi hitam (*black hat hacker*);
4. *Defacing* adalah kegiatan mengubah halaman situs/website pihak lain, seperti yang pernah terjadi pada situs Menkominfo dan Partai Golkar, Bank Indonesia dan Situs KPU saat Pemilu 2004. Tindakan *deface* adalah semata-mata iseng, untuk unjuk kebolehan, pamer kemampuan membuat program namun tak jarang ada juga yang mencuri data-data tertentu untuk kemudian dijual pada pihak lain. Menurut hemat penulis apa-pun nama nya selagi kegiatan tersebut dilakukan secara melawan hak dan menimbulkan kerugian bagi pihak lain, hal tersebut merupakan tindakan yang melawan hukum;
5. *Phising* adalah kegiatan memancing pemakai komputer di Internet (*user*) agar mau memberikan informasi data diri pemakai (*username*) dan kata sandinya (*password*) pada suatu website yang sudah di-*deface*. Phising biasanya diarahkan kepada pengguna *online banking*, isian data pemakai dan *password* yang vital;
6. *Spamming* adalah pengiriman berita atau iklan lewat surat elektronik (*email*) yang tak dikehendakai oleh pemilik *email*, dengan adanya hal ini terkadang menurut pengalaman penulis sebagai pengguna *email* terkadang menjadi gangguan tertentu apalagi spamm tersebut begitu banyaknya;
7. *Malware* adalah program komputer yang mencari kelemahan dari suatu *software*. Umumnya malware diciptakan untuk membobol atau merusak suatu *software* atau *operating*

[24] Antoni, 2017, "Kejahatan Dunia Maya (Cyber Crime) Dalam Simak Online", *Jurnal Nurani*, Vol. 17 No. 2. Hlm 264 - 265

system. *Malware* terdiri dari berbagai macam yaitu: *virus, worm, Trojan horse, adware, browser hijacker* dan lain sebagainya.

Anatomi kejahatan siber berdasarkan Undang - Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang - Undang Nomor 11 Tahun 2008 dapat dibagi menjadi dua kelompok. Pertama, kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Di bawah Undang-Undang Informasi dan Transaksi Elektronik, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan-kejahatan tersebut dianggap sebagai kejahatan kontemporer yang menghasilkan bentuk kejahatan baru.

Jenis Kejahatan	**Ketentuan dalam UNDANG - UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG - UNDANG NOMOR 11 TAHUN 2008**
Meretas (*Hacking*)	Pasal 30
Intersepsi ilegal	Pasal 31 Ayat (1) dan Pasal 31 Ayat (2)
Mengotori (*Defacing*)	Pasal 32
Pencurian Elektronik	Pasal 32 Ayat (2)
Interference	Pasal 33
Memfasilitasi tindak pidana terlarang	Pasal 34
Pencuri Identitas Identitas	Pasal 35

Tabel. 1.

Jenis Kejahatan Siber Kelompok Pertama

Sumber : https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

Kelompok kedua adalah konten ilegal dengan menggunakan internet, komputer dan teknologi terkait untuk melakukan kejahatan. Di bawah UNDANG - UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG - UNDANG NOMOR 11 TAHUN 2008, ada tujuh jenis kejahatan yang diklasifikasikan sebagai kejahatan yang menargetkan internet, komputer, dan teknologi terkait. Kejahatan ini terkait dengan publikasi dan distribusi konten ilegal. Tidak seperti kelompok pertama yang menganggap bentuk kejahatan baru, kelompok kedua dianggap sebagai kejahatan lama, tetapi perkembangan teknologi telah menciptakan media baru untuk memberikan kebebasan berekspresi. Oleh karena itu, legislator mengatur ulang kejahatan dalam Undang-Undang Informasi dan Transaksi Elektronik. Sebenarnya, semua jenis kejahatan ini sudah diatur dalam tindakan kriminal lainnya dan ini menciptakan apa yang disebut Douglas Huzak sebagai kriminalisasi berlebihan.

Jenis Kontent Ilegal	**Ketentuan dalam UNDANG - UNDANG NOMOR 19 TAHUN 2016 TENTANG PERUBAHAN ATAS UNDANG - UNDANG**	**Ketentuan dalam Undang-Undang Lainnya**

	NOMOR 11 TAHUN 2008	
Pornografi	Pasal 27 Ayat (1)	Undang-Undang No. 44 Tahun 2008 tentang Pornografi dan Kitab Undang-Undang Hukum Pidana (KUHP)
Judi	Pasal 27 Ayat (2)	KUHP
Fitnah	Pasal 27 Ayat (3)	KUHP
Pemerasan	Pasal 27 Ayat (4)	KUHP
Tipuan yang membahayakan konsumen	Pasal 28 Ayat (1)	Undang-Undang No. 8 Tahun 1999 tentang Perlindungan Konsumen
Ujaran kebencian	Pasal 28 Ayat (2)	KUHP
Ancaman kekerasan terhadap orang lain	Pasal 29	KUHP

Tabel. 2.

Jenis Konten Ilegal Menurut Undang – Undang ITE

Sumber : https://business-law.binus.ac.id/2019/06/30/konsep-kejahatan-siber-dalam-sistem-hukum-indonesia/

1.5.3 Tinjauan Umum Tentang Keamanan Siber (*Cyber Security*)

1.5.3.1 Pengertian *Cyber Security*

Cyber-security adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna. Organisasi dan aset pengguna dalam *cyber-security* termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem

telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya. *Cyber-security* merupakan upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan aset pengguna terhadap risiko keamanan yang relevan dalam lingkungan *cyber*.[25]

Global cyber-security dibangun di atas lima bidang kerja: Kepastian Hukum (Undang - Undang *Cyber Crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru); Kerjasama Internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*) (Undang-Undang *Cyber Crime*); teknis dan tindakan prosedural (pengguna akhir dan bisnis (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak); struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih); *capacity building* dan pendidikan.[26]

Pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* risiko keamanan yang relevan dalam lingkungan *cyber*. Tujuan keamanan umum terdiri dari: ketersediaan; Integritas termasuk didalamnya keaslian dan kemungkinan upaya mengurangi terjadinya penolakan serta terakhir kerahasiaan.[27]

Keamanan komputer (*computer security*) melingkupi 4 (empat) aspek, yaitu *privacy, integrity, authentication* dan *availability*. Selain keempat aspek itu masih ada 2 (dua) aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic*

[25] Handrini Ardiyanti. "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia". *Jurnal Politica*. Volume 5, Nomor 1, Juni 2014. Hlm. 98

[26] *Ibid.*

[27] *Ibid.*

commerce, yaitu *access control* dan *non- repudiation*. Aspek utama dari *privacy* atau *confidentially* adalah usaha untuk menghindarkan penggunaan informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data yang sifatnya *private*, sedangkan confidentially biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Aspek *integrity* menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi tersebut. Aspek *authentication* berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi tersebut adalah betul-betul orang yang dimaksud. Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. *Access control* berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. Aspek *non-repudiation* ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

Cyber-security lebih lanjut dimaknai sebagai semua mekanisme yang dilakukan untuk melindungi dan meminimalkan gangguan kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*) informasi. Mekanisme ini harus bisa melindungi informasi baik dari physical attack maupun *cyber attack.*

Cyber-security merupakan upaya untuk melindungi informasi dari adanya *cyber attack*, adapun elemen pokok *cyber-security* adalah: [28]

6. Dokumen *security policy* merupakan dokumen standar yang dijadikan acuan dalam menjalankan semua proses terkait keamanan informasi.
7. *Information infrastructure* merupakan media yang berperan dalam kelangsungan operasi informasi meliputi *hardware* dan *software*. Contohnya adalah *router, switch, server, sistem operasi, database, dan website.*
8. *Perimeter Defense* merupakan media yang berperan sebagai komponen pertahanan pada infrastruktur informasi misalnya *IDS, IPS, dan firewall.*
9. *Network Monitoring System* merupakan media yang berperan untuk memonitor kelayakan, utilisasi, dan *performance* infrastruktur informasi.
10. *System Information and Event Management* merupakan media yang berperan dalam memonitor berbagai kejadian di jaringan termasuk kejadian terkait pada insiden keamanan.
11. *Network Security Assessment* merupakan elemen *cyber-security* yang berperan sebagai mekanisme kontrol dan memberikan *measurement level* keamanan informasi.
12. *Human resource dan security awareness* berkaitan dengan sumber daya manusia dan *awareness*-nya pada keamanan informasi.

Selain *cyber-security* kelangsungan operasi informasi juga bergantung pada *physical security* yang tentunya berkaitan dengan semua elemen fisikal misalnya bangunan data *center, disaster recovery system*, dan media transmisi.

Ada beberapa hal yang harus dilindungi dalam sebuah sistem jaringan informasi global berbasis internet (*cyberspace*), yaitu:[29]

1. Isi/substansi data dan/atau informasi yang merupakan *input* dan *output* dari penyelenggara sistem informasi dan disampaikan kepada publik atau disebut juga dengan *content*.

[28] *Ibid*, hlm. 99

[29] Dr. Darmawan Napitula, S.T., M.Kom. "Kajian Peran *Cyber Law* Dalam Memperkuat Keamanan Sistem Informasi Nasional". *Jurnal Kriminologi*. Volume 1, Nomor 1, 2017. Hlm. 105

Dalam hal penyimpanan data dan /atau informasi tersebut akan disimpan dalam bentuk data base dan dikomunikasikan dalam bentuk data *messages*;

2. Sistem pengolahan informasi (*computing and/or information system*) merupakan jaringan sistem informasi organisasional yang efisien, efektif dan legal. Dalam hal suatu sistem informasi merupakan perwujudan penerapan perkembangan teknologi informasi ke dalam suatu bentuk organisasional /organisasi perusahaan (bisnis);
3. Sistem komunikasi (*communication*) merupakan perwujudan dari sistem keterhubungan (*interconnection*) dan sistem pengoperasian global (*inter operation*al) antar sistem informasi /jaringan komputer (*computer network*) maupun penyelenggaraan jasa dan/atau jaringan telekomunikasi; dan
4. Masyarakat (*community*) sebagai subyek atau pengguna Internet.

Menjaga keempat aspek tersebut merupakan bagian dari *policy* keamanan sistem informasi. Keamanan sistem informasi berbasis internet merupakan suatu keharusan yang harus diperhatikan karena jaringan komputer internet sifatnya publik dan global pada dasarnya tidak aman. Sistem keamanan jaringan komputer yang terhubung ke internet harus direncanakan dan dipahami dengan baik agar informasi yang berharga itu dapat terlindungi secara efektif. Untuk mencapai semua itu, jaringan komputer harus dianalisis sehingga

diketahui apa yang harus dan untuk apa diamankan, serta seberapa besar nilainya.

Keamanan komputer (*computer security*) melingkupi 4 (empat) aspek, yaitu *privacy, integrity, authentication* dan *availability*.[30] Selain keempat aspek itu masih ada 2 (dua) aspek lain yang juga sering dibahas dalam kaitannya dengan *electronic commerce*, yaitu *access control* dan *non- repudiation*. Aspek utama dari *privacy* atau *confidentially* adalah usaha untuk menghindarkan penggunaan informasi dari orang yang tidak berhak mengakses. *Privacy* lebih ke arah data yang sifatnya *private*, sedangkan *confidentially* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Aspek *integrity* menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi tersebut. Aspek *authentication* berhubungan dengan metode untuk menyatakan bahwa informasi betul-betul asli atau orang yang mengakses atau memberikan informasi tersebut adalah betul-betul orang yang dimaksud. Aspek *availability* atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. *Access control* berhubungan dengan cara pengaturan akses pada informasi. Hal ini biasanya berhubungan dengan masalah *authentication* dan juga *privacy*. Aspek non-repudiation ini menjaga

[30] *Ibid*. Hlm. 106

agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi.

1.5.3.2 Kebijakan *Cyber Security* di Indonesia

Kebijakan *cyber-security* secara khusus di Indonesia telah diinisiasi sejak tahun 2007 dengan dikeluarkannya Peraturan Menteri Komunikasi dan Informatika No.26/ PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol *Internet* yang kemudian direvisi dengan Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2017 tentang Perubahan Keempat atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol *Internet*. Salah satu yang diatur dalam peraturan tersebut adalah pembentukan ID-SIRTII, yang merupakan kepanjangan dari *Indonesia Security Incident Response Team on Internet Infrastructure* adalah Tim yang ditugaskan Menteri Komunikasi dan Informatika (Kominfo) untuk membantu pengawasan keamanan jaringan telekomunikasi berbasis protokol internet. Tugas dan fungsi dari ID-SIRTII diantaranya melakukan pemantauan, pendeteksian dini, peringatan dini terhadap ancaman dan gangguan pada jaringan, berkoordinasi dengan pihak-pihak terkiat di dalam maupun luar negeri di dalam menjalankan tugas pengamanan jaringan telekomunikasi berbasis protokol internet, mengoperasikan, memelihara dan mengembangkan sistem

database sistem IDSIRTII, menyusun katalog-katalog dan silabus yang berkaitan dengan proses pengamanan pemanfaatan jaringan, memberikan layanan informasi atas ancaman dan gangguan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet, menjadi contact point dengan lembaga terkait tentang keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet serta menyusun program kerja dalam rangka melaksanakan pekerjaan yang berkaitan dengan keamanan pengamanan pemanfaatan jaringan telekomunikasi yang berbasis protokol internet.[31] Terkait dengan upaya menjamin kepastian hukum dalam pengembangan *cyber-security* telah dilakukan antara lain dengan melaksanakan serangkaian program yang sudah mulai berjalan diantaranya: menginisiasi peraturan perundangundangan yang terkait dengan *cyber-security* seperti Undang–Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Peraturan Pemerintah tentang Penyelenggaraan Sistem dan Transaksi Elektronik No. 82 Tahun 2012, menyusun kerangka nasional *cyber-security.*[32]

1.5.3.3 Pendekatan Penal dan Non Penal dalam Keamanan Siber

Pendekatan penal merupakan cara memanfaatkan sarana

[31]Pasal 9 Peraturan Menteri Komunikasi dan Informatika No. 29/PER/M.KOMINFO/12/2010 tentang perubahan kedua Peraturan Menteri Komunikasi dan Informatika No. 26/PER/M.Kominfo/5/2007 tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol Internet.

[32] Handrini Ardiyanti. "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia". *Jurnal Politica*. Volume 5, Nomor 1, Juni 2014. Hlm. 100

pidana atau sanksi pidana. Pertanyaan ini berkaitan dengan bidang politik hukum pidana (*penal policy*), yaitu bagaimana sebaiknya hukum pidana itu dibuat, disusun dan digunakan untuk mengatur atau mengendalikan tingkah laku manusia dalam masyarakat. khususnya guna menanggulangi kejahatan yang dilakukan baik oleh anggota masyarakat maupun oleh penguasa.

Terkait dengan kejahatan siber, perlu diingat kembali bahwasannya sifat dari kejahatan ini sendiri adalah *anonymity*. Media siber (*Internet*) memberikan kemudahan bagi pelaku kejahatan siber karena pada hakikatnya pelaku tidak mudah terungkap atau terdeteksi dan ditelusuri, dan menggunakan ruang-ruang *chatting, facebook*, maupun forum diskusi terbuka lainnya.[33]

Teori pendekatan penal dan nonpenal pada kasus data pribadi berkaitan dengan cara hukum mengatur dan menegakkan hukum terkait dengan pengumpulan, penggunaan, dan perlindungan data pribadi seseorang. Kebijakan penal dalam konteks ini berarti penggunaan hukum pidana untuk menghukum pelanggaran terhadap privasi data pribadi seseorang. Ini dapat mencakup tindakan seperti pencurian identitas, peretasan, atau penggunaan data pribadi tanpa izin atau persetujuan yang sah.

Di sisi lain, kebijakan nonpenal pada kasus data pribadi berfokus pada pengaturan dan pengawasan pengumpulan dan

[33] Hardianto Djanggih. "Konsepsi Perlindungan Hukum Bagi Anak sebagai Korban Kejahatan Siber Melalui Pendekatan Penal dan Non Penal", *Jurnal Mimbar Hukum*, Volume 30, Nomor 2, Juni 2018. Hlm. 321.

penggunaan data pribadi oleh pihak-pihak tertentu, seperti perusahaan atau organisasi. Ini dapat mencakup undang-undang privasi data yang memerlukan perusahaan untuk meminta persetujuan dari pemilik data pribadi sebelum mengumpulkan atau menggunakan data tersebut, serta memerlukan perusahaan untuk melindungi data pribadi tersebut dari akses yang tidak sah atau penyalahgunaan.

Dalam praktiknya, kebijakan penal dan nonpenal sering digunakan bersama-sama untuk memastikan perlindungan data pribadi yang efektif. Pemerintah dapat menggunakan hukum pidana untuk menegakkan undang-undang privasi data yang ada dan memastikan bahwa pelanggar hukum dikenakan sanksi yang sesuai, sementara undang-undang privasi data yang diterapkan dengan benar dapat membantu mencegah pelanggaran privasi data yang dapat mengarah pada tindakan pidana. Upaya penanggulangan kejahatan tidak hanya dengan sarana "penal" yang bersifat represif (penindakan / pemberantasan), tetapi juga dilakukan dengan sarana non penal (bukan/diluar hukum pidana), yang bersifat prefentif (pencegahan/penangkalan/pengendalian). Pendekatan non penal memiliki tujuan utama untuk memperbaiki kondisikondisi sosial tertentu, namun secara tidak langsung mempunyai pengaruh preventif terhadap kejahatan.[34]

[34] *Ibid*, hlm. 325

1.6 Metode Penelitian

1.6.1 Jenis Penelitian

Salah satu yang terpenting dalam penulisan karya ilmiah terletak pada metode penelitian yang di gunakan, dengan demikian dalam penelitian wajib diterapkan metode yang tepat sebab hal itu adalah panduan penting untuk melakukan penelitian,dan khususnya analisis yang berkenaan dengan bahan penelitian. Dalam hal melakukan penelitian hukum yang di maksud sebagai upaya untuk mengembangkan suatu hukum, penelitian hukum mempunyai peranan sangat penting, dikarenakan jika tidak terdapat suatu penelitian hukum yang baik dan berkualitas, maka tidak dapat mengembangkan secara optimal dan semestinya.[35] Karena itu, masyarakat dapat menemukan jawaban atau solusi terkait dengan berbagai isu isu hukum yang terdapat pada kehidupan masyarakat dengan semestinya. Penulisan Skripsi ini di terapkan menggunakan Metode Penelitian Hukum dengan tujuan menelusuri, mempelajari serta mengolah bahan bahan hukum yang di dapatkan dengan tujuan mendapatkan kesimpulan dan menjawab isu hukum yang sinkron dengan kebenaran ilmiah secara teoritis atau praktis.[36]

Dalam penulisan skripsi ini menggunakan jenis Penelitian yuridis Normatif.[37] Penelitian yuridis Normatif pada umumnya dikenal dengan

[35] Dyah Ochtorina Susanti dan Aan Efendi, *Penelitian Hukum: Legal Research* (Jakarta: Sinar Grafika, 2015), hlm 7.

[36] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana Prenamedia Group, 2016), hlm. 18.

[37] Soerjono Soekanto, Sri Mamudji, *Penelitian Hukum Normatif* (Rajawali Press, Jakarta, 2010). Hlm. 12.

Penelitian Hukum Doktrinal. Dalam Penelitian skripsi ini Hukum dijadikan konsep menjadi sesuatu yang ditulis dalam Peraturan Perundang-Undangan (*law in books*) atau mengkonsepkan Hukum sebagai Norma yang merupakan patokan berprilaku manusia.[38]

1.6.2 Sumber Data

Pada penelitian ini, bahan hukum menjadi bagian penting dalam penelitian hukum. Hal ini dikarenakan bahan hukum merupakan bahan yang digunakan untuk menjawab isu hukum atau topik dalam bahasan penelitian. Bahan hukum pada penelitian ini dibagi menjadi 3 (tiga), yaitu Bahan Hukum Primer, Bahan Hukum Sekunder dan Bahan Hukum Tersier.[39] Adapun Bahan Hukum yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Bahan Hukum Primer

Bahan hukum dibagi menjadi Peraturan Perundang-Undangan, Berita Acara, Putusan Pengadilan dan Dokumen Resmi Negara. Menurut Dyah Ochtorina Susanti dan A'an Efendi "Bahan hukum primer yang bersifat mandatory authority yang terdiri dari Peraturan Perundang-Undangan yang dikeluarkan diwilayah hukumnya sendiri serta Putusan Hakim".

Selanjutnya Bahan Hukum Premier bersifat persuasive authority yaitu bahan hukum yang meliputi Peraturan Hukum Perundang-Undangan di wilayah Hukum Negara lain, namun

[38] Amirudin dan Zainal Asikin, *Pengantar Metode Penelitian Hukum* (Raja Grafindo Persada, Jakarta, 2016). hlm. 118

[39] Dyah Ochtorina Susanti dan A'an Efendi. *Op.cit*, hlm.89

berkaitan dengan sesuatu yang sama dengan Putusan Hakim di wilayah yuridiksi negara lain. Penulis menggunakan Bahan Hukum Primer yaitu:

- Kitab Undang-Undang Hukum Pidana (KUHP);
- Kitab Undang-Undang Hukum Acara Pidana (KUHAP);
- Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 Tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.
- Undang-Undang Republik Indonesia Nomor 24 Tahun 2013 perubahan atas Undang-Undang Nomor 23 Tahun 2006 Tentang Administrasi Kependudukan.
- Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi
- Peraturan Pemerintah Republik Indonesia Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Teransaksi Elektronik
- Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 Tentang Perlindungan Data Pribadi Dalam Sistem Elektronik
- Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2017 tentang Perubahan Keempat atas Peraturan Menteri Komunikasi dan Informatika Nomor 26/PER/M.KOMINFO/5/2007 Tentang Pengamanan Pemanfaatan Jaringan Telekomunikasi Berbasis Protokol

Internet

- Putusan Pengadilan (PN) Medan Nomor 541/Pid.Sus/2022/PN Mdn
- Putusan Pengadilan (PN) Bireuen Nomor 54/Pid.Sus/2022/Pn Bir

b. Bahan Hukum Sekunder

Bahan hukum yang terdiri atas Buku atau Jurnal Hukum berisi Prinsip-Prinsip Dasar (Asas Hukum), Pandangan para Ahli Hukum (Doktrin) dan Hasil Penelitian Hukum Tesis (S2), Skripsi (S1) yang ada sangkut pautnya dengan penelitian skripsi ini.[40]

c. Bahan Hukum Tersier

Bahan Hukum yang menerangkan penjelasan mengenai Bahan Hukum Primer serta Bahan Hukum Sekunder yaitu : Kamus (hukum); Majalah Hukum; Kamus Besar Bahasa Indonesia; Kamus Lengkap Bahasa Inggris-Bahasa Indonesia..

1.6.3 Metode Pengumpulan Data

Untuk memperoleh bahan hukum yang diperlukan dalam penelitian proposal skripsi ini diperoleh dengan cara studi pustaka atau dokumen. Studi dokumen merupakan tahap awal dari setiap kegiatan penulisan hukum. Studi dokumen bagi penelitian hukum yakni meliputi studi bahan-bahan hukum yang terdiri dari bahan hukum primer, bahan hukum sekunder, serta bahan hukum tersier. Data kepustakaan yang diperoleh melalui penelitian kepustakaan yang bersumber dari

[40] *Ibid.* Hlm. 89

peraturan perundang-undangan, buku, dokumen resmi, publikasi, serta hasil penelitian. Studi kepustakaan bagi penelitian hukum normatif, merupakan metode pengumpulan data yang membahas doktrin-doktrin atau asas-asas dalam ilmu hukum.

1.6.4 Metode Analisis Data

Metode analisis data merupakan tahap dalam suatu penelitian, karena dengan analisis data ini, data yang diperoleh akan diolah untuk mendapatkan jawaban dari permasalahan yang ada. Data yang diperoleh terlebih dahulu diolah, kemudian dianalisis secara kualitatif dengan memperhatikan ketentuan hukum yang ada dan asas-asas hukum yang berkaitan dengan kaidah hukum yang berlaku sehingga menghasilkan uraian yang bersifat deskriptif kualitatif yaitu teknik yang menggambarkan dan menginterprestasikan arti data-data yang telah terkumpul dengan memberikan perhatian dan merekam sebanyak mungkin aspek situasi yang diteliti pada saat itu, sehingga memperoleh gambaran secara umum dan menyeluruh mengenai keadaan sebenarnya.[41]

1.6.5 Lokasi Penelitian

Lokasi penelitian adalah tempat atau daerah yang dipilih sebagai tempat pengumpulan data untuk menemukan jawaban atau masalah. Lokasi yang dipilih sebagai penelitian yakni perpustakaan fakultas hukum, perpustakaan universitas atau perpustakaan daerah, dan Kejaksaan Negeri Sidoarjo sebagai keperluan untuk validasi data dan

[41] *Ibid*. hlm. 122

wawancara singkat. Waktu penelitian ini adalah 3 (tiga) bulan, dimulai dari bulan Juni 2022 sampai bulan Agustus 2022. Penelitian ini mulai dilaksanakan pada bulan Mei 2022 yang meliputi tahap persiapan penelitian yakni pendaftaran proposal, penentuan dosen pembimbing, pengajuan judul, acc judul, pencarian data, penulisan penelitian, bimbingan proposal penelitian, pendaftaran ujian proposal, seminar proposal, dan perbaikan proposal. Kemudian dimulai dari bulan November hingga Maret 2023, dilanjutkan dengan bimbingan skripsi hingga ACC Skripsi untuk mengikuti Ujian/Sidang Seminar Hasil Akhir Skripsi.

1.6.6 Sistematika Penulisan

Untuk mempermudah proposal skripsi ini, maka kerangka dibagi menjadi beberapa bab yang terdiri dari beberapa sub bab. Proposal skripsi ini dengan judul **"KAJIAN YURIDIS TINDAK PIDANA PEMALSUAN IDENTITAS DATA DIRI DALAM SITUS BANTUAN PRAKERJA".** Dalam pembahasannya dibagi menjadi IV (empat) bab, sebagaimana diuraikan secara menyeluruh tentang pokok permasalahan yang akan dibahas dalam proposal skripsi ini.

Bab pertama, berisi pendahuluan. Dalam bab pertama dibagi dalam beberapa sub bab. Sub bab pertama adalah latar belakang, sub bab kedua adalah rumusan masalah, sub bab ketiga adalah tujuan penelitian, sub bab keempat adalah manfaat penelitian, sub bab kelima adalah kajian pustaka dan sub bab keenam adalah metode penelitian.

Bab kedua, membahas perumusan masalah yang pertama yaitu

apa yang menjadi alasan terjadinya transaksi jual beli data pribadi dalam situs bantuan kartu Prakerja. Dalam bab ini terdiri dari 2 sub bab yaitu dalam sub bab pertama mengenai apa yang menjadi alasan terjadinya transaksi jual beli data pribadi dalam situs bantuan kartu Prakerja dan sub bab kedua membahas terkait perbandingan pengaturan sehingga munculnya kelemahan peraturan atau tinjauan yuridis dalam perlindungan data diri.

Bab ketiga, membahas perumusan masalah yang kedua yaitu bagaimana perlindungan bagi pemilik identitas data diri yang dipalsukan dalam situs bantuan kartu Prakerja. Dalam bab ini menjelaskan tentang bagaimana bentuk perlindungan bagi pemilik identitas data diri yang disalahgunakan oleh oknum tertentu untuk kepentingan pribadinya berdasarkan Undang – Undang Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi.

Bab keempat, berisi penutup bagian terakhir penulisan skripsi ini yang berisi kesimpulan dari pembahasan yang telah diuraikan dalam bab-bab sebelumnya dan juga berisikan saran saran dari penulis. Dengan demikian bab penutup ini merupakan bagian akhir dari penulisan proposal skripsi ini, sekaligus merupakan rangkuman jawaban atas permasalahan yang diangkat dalam penulisan skripsi ini.