

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Globalisasi di era milenium saat ini telah membawa pengaruh yang besar kepada seluruh sektor kehidupan manusia, khususnya dalam bidang teknologi dan internet. Teknologi dan internet memiliki peran yang sangat besar dalam menunjang segala aktivitas kehidupan manusia. Dengan ditemukannya internet maka dapat memungkinkan kita melakukan pertukaran informasi dengan siapapun dan dimanapun orang tersebut berada tanpa dibatasi oleh ruang dan waktu. Perkembangan teknologi informasi utamanya *interconnection-networking* (internet) membawa perubahan di seluruh lini kehidupan manusia.

Pada periode tahun 2022-2023, berdasarkan hasil survei Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) pengguna internet di Indonesia mencapai 215, 63 (dua ratus lima belas koma enam puluh tiga) juta orang.¹ Data tersebut menunjukkan bahwa pemanfaatan teknologi digital di Indonesia sangat besar dan tentu saja memberikan dampak bagi beberapa sektor salah satunya adalah dalam hal sektor bisnis atau industri-industri bisnis. Perkembangan kegiatan bisnis di Indonesia menimbulkan banyak kalangan pengusaha tidak lagi bertindak sendiri dalam menjalankan usahanya, melainkan mereka bersama-sama mendirikan persekutuan-

¹ Asosiasi Penyelenggara Jasa Internet Indonesia, “Survei APJII Pengguna Internet di Indonesia Tembus 215 Juta Orang”. <https://apjii.or.id/berita/d/survei-apjii-pengguna-internet-di-indonesia-tembus-215-juta-orang>, diakses pada 22 May 2023, hal. 1

persekutuan atau perseroan-perseroan diantaranya adalah persekutuan perdata, perseroan terbatas, persekutuan komanditer, firma dan koperasi.² Di dalam menjalankan suatu badan usaha hal terpenting yang harus dapat dilakukan adalah mengenai perizinan dan legalitas dari badan usaha tersebut.

Legalitas akan suatu perusahaan merupakan hal penting karena dengan mengesahkan suatu badan usaha maka perusahaan tersebut dapat diakui oleh negara dan masyarakat pada umumnya. Legalitas perusahaan harus sah menurut peraturan perundang-undangan dimana perusahaan tersebut dilindungi atau dipayungi dengan berbagai dokumen hingga sah dimata hukum pada pemerintahan saat itu.³ Legalitas dapat diwujudkan pada kepemilikan izin suatu badan usaha dalam menjalankan usahanya. Dengan adanya suatu perizinan yang sesuai dengan bidang usaha tersebut, maka suatu badan usaha tersebut dapat menjalankan aktivitas bisnisnya dengan lancar. Badan usaha harus melakukan beberapa prosedur yang telah ditetapkan oleh pemerintah untuk mendapatkan suatu legalitas sesuai dengan peraturan yang berlaku di Indonesia.

Berbagai manfaat akan bisa diperoleh dengan adanya suatu legalitas, maka dari itu penting bagi setiap badan usaha untuk memiliki legalitas dalam menjalankan setiap usahanya. Dalam kenyataannya, legalitas yang harus diperoleh suatu perusahaan sering kali dihadapkan dengan berbagai

² C.S.T. Kansil, *Pokok-Pokok Pengetahuan Hukum Dagang Indonesia*, (Jakarta: Sinar Grafika, 1992), hal. 68

³ Janus Sidabalok, *Hukum Perusahaan: Analisis terhadap Pengaturan Peran Perusahaan Dalam Pembangunan Ekonomi Nasional di Indonesia*, (Bandung: CV. Nuansa Aulia, 2012), hal. 12

hambatan, salah satunya adalah dalam hal pengurusan perizinan. Perizinan adalah salah satu bentuk pelaksanaan fungsi pengaturan dan bersifat pengendalian yang dimiliki oleh pemerintah terhadap kegiatan-kegiatan yang dilakukan oleh masyarakat. Perizinan bertujuan untuk mengendalikan setiap kegiatan atau perilaku individual kolektivitas yang bersifat preventif. Perizinan dapat berbentuk pendaftaran, rekomendasi, sertifikasi, penentuan kuota, dan izin untuk melakukan suatu usaha yang biasanya harus dimiliki atau diperoleh suatu perusahaan atau seseorang sebelum yang bersangkutan dapat melakukan suatu kegiatan atau tindakan.⁴

Dalam hal pengurusan perizinan terkadang muncul beragam hambatan diantaranya adalah proses perizinan yang cukup lama serta berbagai hambatan lain yang dapat menghambat roda perekonomian. Namun sejalan dengan teknologi yang semakin berevolusi maka perizinan juga mengikuti jalannya perkembangan tersebut. Dengan adanya perkembangan zaman yang berbasis digital maka timbul suatu sistem perizinan elektronik yang dapat memudahkan pengurusan perizinan. Salah satu upaya pemerintah untuk mengikuti perkembangan era digital saat ini ialah dengan menerbitkan Peraturan Pemerintah Nomor 24 Tahun 2018 Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik (“PP 24/2018”). Dengan peraturan tersebut pemerintah Indonesia berupaya meningkatkan efisiensi kegiatan usaha dengan percepatan pelaksanaan berusaha yang disusun dalam peraturan tersebut.

⁴ Adrian Sutedi, *Hukum Perizinan: Dalam Sektor Pelayanan Publik*, (Jakarta: Sinar Grafika, 2010, hal 2

Pengurusan perizinan yang diatur dalam peraturan pemerintah tersebut memudahkan para pelaku usaha khususnya badan usaha untuk mengurus legalitas agar dapat menjalankan usahanya. Dari kebijakan tersebut, semua pelayanan perizinan usaha menjadi terintegrasi oleh pusat melalui 1 (satu) Sistem Perizinan Berusaha Secara Elektronik *Online Single Submission* (“OSS”). Dengan sistem pelayanan berusaha terintegrasi secara elektronik, maka semua pengurusan izin usaha bisa dilakukan dengan cara yang lebih mudah, cepat, tepat dan efisien. Sistem OSS diharapkan dapat mewujudkan proses perizinan yang lebih sederhana dan praktis yang berdampak positif bagi iklim investasi dunia bisnis di Indonesia. Dengan pengaturan tersebut diharapkan sistem ini dapat memberikan kemudahan kepada pelaku usaha untuk mengurus perizinan dan memudahkan pengawasan pemerintah akan badan usaha tersebut.

Pada tahun 2020 dengan berlakunya Undang-Undang Nomor 11 Tahun 2020 tentang Cipta Kerja sebagai peraturan pelaksanaannya terbit 49 peraturan pemerintah dan juga 4 peraturan presiden salah satunya adalah Peraturan Pemerintah Nomor 5 Tahun 2021 tentang Perizinan Berusaha Berbasis Resiko (“PP 5/2021”). Peraturan Pemerintah Nomor 5 Tahun 2021 ini melahirkan sistem elektronik pelayanan perizinan yang baru yaitu OSS *Risk Basic Approach* (“OSS RBA”) sebagai entitasnya. Layanan digital OSS diharapkan dapat menciptakan cara kerja dan arah kebijakan baru dalam reformasi layanan perizinan usaha di negeri ini.⁵

⁵ *Ibid*, hal 5.

Di dalam proses pendaftaran izin berusaha pengguna harus melakukan tahap pertama yang dimulai dengan pembuatan Nomor Induk Berusaha (NIB). Kemudian pengguna harus memasukkan identitas diri yang wajib diinput, jika tidak terisi maka pendaftaran tidak dapat berlanjut ke tahap selanjutnya. Data pribadi tersebut berisikan identitas diri nama, NIK dan alamat email serta data-data pribadi lainnya. Data-data yang harus diisi tersebut akan tersimpan dalam sistem OSS. Di dalam pelaksanaan tersebut terdapat pihak-pihak yang diberikan akses terhadap OSS salah satunya adalah Badan Koordinasi Penanaman Modal (“BKPM”) untuk pemerintah pusat dan Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu (“DPMPTSP”) provinsi ataupun kabupaten/kota untuk Pemerintah Daerah.

Data pribadi adalah data yang berupa identitas kode, simbol, huruf atau angka penanda personal seseorang yang bersifat pribadi dan rahasia. Data merupakan aset yang berharga terkhususnya bagi subjek data baik perseorangan maupun korporasi yang terus menerus mengumpulkan, bertukar, mengolah, menyimpan data.⁶ Pengendali data dalam sistem OSS mencakup beberapa pihak yang diberikan akses sebagai pengelola data terhadap OSS ini di antaranya yaitu BKPM yang dikhususkan pemerintah pusat dan DPMPTSP yang dikhususkan pemerintah daerah baik provinsi maupun kabupaten kota.

⁶ Suisno, A. D. N., “Urgensi Hukum Telematika Dalam Perlindungan Data Pribadi”, *Jurnal Independent*, Vol. 1, No. 8 (2020), hal 265-272

Di dalam era ekonomi digital, data pribadi perseorangan merupakan suatu hal yang harus dapat dipertanggungjawabkan karena bertujuan untuk menunjang kepentingan transaksi elektronik seperti melampirkan KTP, NPWP, dan lain sebagainya. Namun ketentuan hukum terkait perlindungan data pribadi di Indonesia sampai saat ini masih bersifat parsial dan sektoral.⁷ Dalam proses pengurusan perizinan yang terintegrasi secara elektronik ini muncul beberapa celah yang sering dimanfaatkan oleh pihak-pihak yang tidak bertanggungjawab. Salah satu yang seringkali disalahgunakan ialah mengenai data badan usaha yaitu data pribadi pengurus dan pemegang saham.

Disamping membawa adanya keefisienan suatu sistem yang terintegrasi secara elektronik tersebut akan memberikan suatu tantangan baru terkhususnya dalam pelaksanaannya yang menggunakan sistem elektronik. Tantangan baru tersebut berkaitan dengan kemungkinan atau potensi terjadinya pelanggaran terhadap perbuatan-perbuatan yang dilarang dalam penggunaan data masyarakat (pengguna) dalam sistem elektronik OSS ini. Dalam hal ini pelanggaran yang dimaksud dapat dikatakan sebagai suatu kejahatan siber.⁸ Pertanggungjawaban dan keamanan akan suatu data pribadi yang diunggah ke dalam platform tersebut harus bisa dilandasi dengan legalitas yang jelas dari suatu badan usaha. Pelindungan tersebut

⁷ RM. Hasbu Pratama Arya Agung, "Perlindungan Data Pribadi Dalam Proses Pengurusan Perizinan Perusahaan Berbasis Elektronik *Online Single Submission* (OSS)", Jurnal Ilmiah Galuh Justisi, Vol. 9, No. 1 Maret 2021, hal. 67-75

⁸ Maskun, *Kejahatan Siber (Cyber Crime) Suatu Pengantar*, (Jakarta: Prenada Media, 2014), hal. 21

penting untuk menciptakan perekonomian yang sehat dan terselenggaranya ketertiban hukum bagi masyarakat.

Keberadaan sistem OSS yang didalamnya termuat banyak data penting dari para pemangku kepentingan membuat sistem ini membutuhkan keamanan dan jaminan dalam pengaturan perlindungan data pribadi penggunanya. Dalam kenyataannya sistem perizinan digital OSS yang telah ada belum secara maksimal mewujudkan terselenggaranya keamanan data pribadi antar penggunanya. Substansi dalam PP 5/2021 tidak mengatur mengenai perlindungan data pribadi pengguna dalam sistem tersebut. Karakteristik OSS yang menggunakan sistem satu pintu (*One Data for All Access*) memungkinkan terjadinya kebocoran pada satu data yang berakibat pada akses-akses lainnya yang terdapat di dalam sistem OSS dengan mudah disalahgunakan. Berkaitan dengan hal tersebut maka pencuri data dapat menyalahgunakan data yang diperolehnya dari sistem OSS tersebut dengan mudah.

Berbagai kasus kebocoran dan penyalahgunaan data pribadi yang terjadi masih menimbulkan berbagai macam problematika yang mengkhawatirkan sejak meningkatnya pemanfaatan elektronik. Di Indonesia pelanggaran terhadap penggunaan data pribadi masih seringkali terjadi. Beberapa kasus yang terjadi sejauh ini adalah kasus Tokopedia yang mengalami kebocoran data sebanyak 12.155.583 akun pengguna pada 17

April 2020.⁹ Selain itu pada sektor pemerintahan terdapat 279 (dua ratus tujuh puluh sembilan) juta data penduduk Indonesia yang terdiri atas NIK, slip gaji, nomor telepon, alamat dan email pengguna dari BPJS Kesehatan yang bocor dan beredar.

Data pribadi seperti NIK, nama, email, nomor telepon merupakan data yang berharga yang seharusnya dapat dipertanggungjawabkan dan dilindungi. Salah satu contoh data yang disalahgunakan adalah kasus pemegang saham Tokopedia yang dibocorkan ke publik oleh KrAsia dimana KrAsia diduga memperoleh data tersebut dari BKPM. Dari contoh tersebut menunjukkan bahwa data pribadi sangat rentan untuk diakses secara bebas oleh orang-orang yang tidak bertanggungjawab. Kasus tersebut mengancam data pribadi yang dimiliki oleh pengguna akses layanan tersebut yaitu para pelaku usaha atau pemegang saham yang ada di Indonesia. Indonesia menjadi negara dengan tingkat kebocoran tertinggi dengan menempati urutan ke-3 sebagai negara dengan jumlah kasus kebocoran data terbanyak di dunia.

Selain itu tercatat dalam beberapa tahun terakhir kasus kebocoran data pribadi di Indonesia terus bergulir dan terjadi sebagai suatu kejadian yang seharusnya dapat diperhatikan lebih lanjut. Dalam sektor perizinan sendiri, pada 2022 lalu terjadi kebocoran data dalam kasus pengurusan Surat Izin Mengemudi (SIM) dimana Kementerian Komunikasi dan Informatika

⁹ CNN Indonesia, “Marak Data Bocor, Butuh Taji UU Data Pribadi”. <https://www.cnnindonesia.com/teknologi/20200707230022-185-522059/marak-data-bocor-butuh-taji-uu-data-pribadi>, diakses pada 25 May 2023

mengakui terdapat kesalahan pengendali data pada pengurusan SIM yang mengakibatkan kebocoran data pada kurang lebih 1,3 (satu koma tiga) miliar data pengguna SIM.¹⁰ Pelindungan data pribadi merupakan hal penting yang harus ditegakkan untuk menjamin adanya suatu keamanan data pribadi bagi pengguna. Pelanggaran data pribadi tidak hanya disebabkan oleh kebocoran data pribadi namun pelanggaran juga bisa terjadi dalam hal pemrosesan data pribadi yang tidak bertanggungjawab. Kenyataannya di Indonesia, sistem OSS ini masih kurang dalam mendukung integrasi data yang dapat memperkuat dan menjamin keamanan data pribadi penggunanya.

Suatu layanan atau pelayanan publik yang dapat diakses oleh banyak pengguna membutuhkan data pribadi tertentu untuk dapat memproses suatu informasi atau memberikan layanan tertentu. Dengan hal tersebut maka terdapat tanggung jawab penyelenggara pelayanan dimana pihak yang bersangkutan harus mengolah, menyimpan, dan melindungi data pribadi pengguna layanan dengan baik dan hati-hati. Kedudukan data pribadi seorang pengguna layanan merupakan suatu hal yang harus bisa dipertanggungjawabkan. Hal ini dikarenakan data pribadi merupakan sekumpulan informasi tertentu mengenai seseorang yang mana hal tersebut memiliki nilai ekonomi sendiri sehingga akan sangat rawan apabila

¹⁰ Kata Data, "Sebut Kominfo Bodoh Soal Data SIM Card HP Bocor, Siapa Hacker Bjorka?". <https://katadata.co.id/desysetyowati/digital/631827e25e145/sebut-kominfo-bodoh-soal-data-sim-card-hp-bocor-siapa-hacker-bjorka>, diakses 25 May 2023

disalahgunakan untuk kepentingan yang tidak berhubungan dengan tujuan penggunaan data pribadi.¹¹

Pelindungan data pribadi merupakan bagian dari pelindungan konstitusional yang menjadi aspek pelindungan keamanan dan ketahanan negara. Dalam Undang-Undang Dasar Negara Republik Indonesia 1945 (“UUD 1945”) Pasal 28G ayat 1 berbunyi bahwa:

“Setiap orang berhak atas pelindungan diri pribadi, keluarga, kehormatan, martabat, dan harta benda yang di bawah kekuasaannya, serta berhak atas rasa aman dan pelindungan dari ancaman ketakutan untuk berbuat atau tidak berbuat sesuatu yang merupakan hak asasi”.

Pasal tersebut menyatakan bahwa penyelenggara negara harus dapat melaksanakan jaminan pelindungan atas pribadi khususnya dalam pelindungan data pribadi pada setiap orang. Apabila suatu data pribadi pengguna mengalami kebocoran atau akses yang tidak sah dan/atau melawan hukum maka dapat dinyatakan bahwa pengendali data pribadi yang bersangkutan telah gagal untuk melakukan pelindungan terhadap data pribadi yang dipertanggungjawabkan.

Peraturan mengenai pelindungan data pribadi di Indonesia telah mengalami berbagai evolusi. Pelindungan data pribadi di Indonesia nyatanya sudah diatur dalam berbagai peraturan perundang-undangan yaitu Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan sebagaimana telah diubah dengan dengan Undang-Undang Nomor 10 Tahun 1998

¹¹ Tejomurti, *et.all*, “*Legal Protection For Urban Online Transportation User’s Personal Data Disclosure In the Age Of Digital Technology*”, *Padjajaran Journal of Law*, Vol. 5, No. 3, (2018), hal. 485-505

tentang Perbankan. Pelaksanaan elektronik juga diatur dalam undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (“UU ITE”) mengatur perbuatan-perbuatan yang dilarang dalam penggunaan data pribadi termasuk sistem elektronik. Dalam Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik juga mengatur jaminan akan perlindungan data dalam sistem elektronik. Pertanggungjawaban akan sistem OSS masih sulit untuk ditegakkan dikarenakan sistem ini merupakan layanan yang dipegang pemerintah dan suatu sistem terpadu satu pintu yang mengatasmakan berbagai lembaga sebagai pihak ketiga dalam layanan publik.

Pada awalnya pengaturan mengenai perlindungan data pribadi tidak didasari dengan payung hukum yang jelas. Pelindungan data pribadi menjadi suatu hal yang tidak dilandasi dengan landasan hukum yang kuat yang dapat menjamin perlindungan data pribadi warganya. Oleh karena itu banyak pihak-pihak yang menghendaki akan adanya regulasi hukum dalam bentuk undang-undang yang mengatur perlindungan data pribadi seseorang salah satunya dengan menyusun Rancangan Undang-Undang Pelindungan Data Pribadi atau RUU PDP. RUU PDP telah diinisiasi sejak 2016 lalu dan menjadi prioritas untuk dibahas di DPR pada tahun 2019. Dalam prosesnya RUU PDP ini banyak menuai pro dan kontra dan bahkan harus melalui proses yang rumit dan panjang. Hingga pada akhirnya RUU PDP telah

diresmikan menjadi Undang-Undang dalam Rapat Paripurna DPR RI pada 21 September 2022.

Dengan demikian, saat ini di Indonesia telah memiliki peraturan yang mengatur tentang perlindungan data pribadi Warga Negara Indonesia yang tertuang dalam Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi (“UU PDP”). UU PDP mengatur mengenai peraturan yang lebih khusus terkait dengan perlindungan data pribadi. UU PDP mengatur perbuatan-perbuatan apa saja yang dilarang yang dapat merugikan data pribadi seseorang. Penyalahgunaan data yang dilakukan oleh oknum tidak bertanggung jawab dengan menggunakan data dari sistem OSS merupakan suatu perbuatan melawan hukum yang harus bisa ditangani. Namun penerapan tersebut sulit tegakkan dalam realitanya karena sistem OSS merupakan layanan yang dipegang oleh pemerintah dan suatu sistem terpadu satu pintu yang mengatasmakan berbagai lembaga sebagai pihak ketiga dalam layanan publik.

Dengan melihat fenomena tersebut, penulis tertarik untuk menganalisis lebih mengenai perlindungan data pribadi pengguna layanan akses perizinan OSS. Beranjak dari pemikiran yang penulis sampaikan di atas, bahwa masih banyak kekurangan dan potensi pelanggaran penggunaan data pribadi pengguna dalam layanan akses perizinan berbasis elektronik pada OSS maka Penulis melakukan penelitian dalam bentuk skripsi yang berjudul **“OPTIMALISASI PELINDUNGAN DATA PRIBADI PENGGUNA LAYANAN AKSES PERIZINAN *ONLINE SINGLE***

SUBMISSION MELALUI UNDANG-UNDANG NOMOR 27 TAHUN 2022 TENTANG PELINDUNGAN DATA PRIBADI

1.2. Rumusan Masalah

Berdasarkan penjelasan latar belakang masalah di atas, maka Penulis merumuskan rumusan masalah sebagai berikut:

1. Bagaimana kebijakan dan pengaturan data pribadi pengguna layanan akses perizinan usaha dalam layanan OSS ditinjau menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi?
2. Bagaimana kemanfaatan hukum pelindungan data pribadi dalam layanan OSS?

1.3. Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka adapun tujuan dari penelitian yang ingin dicapai adalah sebagai berikut:

1. Untuk melakukan pengembangan ilmu hukum ke depan mengenai kebijakan dan pengaturan data pribadi pengguna layanan akses perizinan usaha dalam layanan OSS ditinjau menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi.
2. Untuk melakukan penemuan hukum mengenai kemanfaatan hukum pelindungan data pribadi dalam layanan OSS.

1.4. Manfaat Penelitian

Adapun kemudian penelitian ini diharapkan memberikan hasil yang dapat bermanfaat sebagai berikut:

1. Manfaat Teoritis

Secara teoritis, penelitian ini diharapkan dapat bermanfaat bagi bidang studi ilmu hukum serta perkembangan hukum nasional di Indonesia yang dapat melindungi data pribadi pengguna layanan akses perizinan OSS.

2. Manfaat Praktis

Secara praktis, diharapkan dengan adanya penelitian ini dapat menjadi solusi untuk menemukan kemanfaatan hukum dalam layanan akses perizinan OSS.

1.5. Sistematika Penulisan

Adapun sistematika penulisan penelitian ini terdiri dari 5 (lima) bab, yaitu:

BAB I PENDAHULUAN

Bab I berisi pendahuluan yang mana terbagi atas 5 (lima) bagian, yaitu latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian serta sistematika penelitian.

BAB II TINJAUAN PUSTAKA

Bab II terbagi atas 2 (dua) bagian besar yang meliputi tinjauan teori dan tinjauan konseptual. Tinjauan teori mencakup teori-teori hukum yang relevan serta berkaitan dengan isu dan permasalahan hukum yang dibahas di dalam penelitian ini. Sementara itu, tinjauan konseptual mencakup konsep-konsep yang menjadi dasar pemikiran yang digunakan pada analisis rumusan masalah.

BAB III METODE PENELITIAN

Bab III memaparkan mengenai metode pendekatan yang menjadi landasan pada penelitian ini, yaitu metode pendekatan, jenis penelitian, tipe penelitian, sumber dan jenis data, teknik pengumpulan data dan teknik analisis data.

BAB IV HASIL PENELITIAN DAN ANALISIS

Bab IV akan menguraikan 2 (dua) hal penting yang berhubungan dengan rumusan masalah yang telah dipaparkan sebelumnya, yaitu: (1) pengaturan data pribadi pengguna layanan akses perizinan data pribadi dalam layanan *Online Single Submission* ditinjau menurut Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi; dan (2) pertanggungjawaban hukum bagi pemerintah terhadap pencegahan penyalahgunaan data pribadi data pengguna layanan akses perizinan *Online Single Submission*

BAB V PENUTUP

Bab V adalah bab terakhir yang akan berisi tentang kesimpulan serta saran yang akan Penulis berikan terkait dengan penelitian yang Penulis telah lakukan.