Healthy Living / Produk
Hukum dan Penegakannya

HALAMAN JUDUL LAPORAN

PENELITIAN KOMPETITIF

PERAN PENYELENGGARA JASA TELEKOMUNIKASI DALAM UPAYA PENCEGAHAN DAN PENANGGULANGAN TINDAK PIDANA PENIPUAN ONLINE DI KOTA SURABAYA

Anton Hendrik S., S.H., M.H. (NPK: 215020)

Dr. Go Lisanawati, S.H., M.Hum. (NPK: 204023)

Natalia Wijaya (NRP: 120114040)

UNIVERSITAS SURABAYA

September, 2018

HALAMAN PENGESAHAN

Judul Penelitian	: **PERAN PENYELENGGARA JASA TELEKOMUNIKASI DALAM UPAYA PENCEGAHAN DAN PENANGGULANGAN TINDAK PIDANA PENIPUAN ONLINE DI KOTA SURABAYA**
Nama Rumpun Ilmu	: Ilmu Hukum
Ketua Peneliti	
a. Nama Lengkap	: Anton Hendrik Samudra, S.H., M.H.
b. NPK/ NIDN	: 215020/0706018403
c. Jabatan Fungsional	: AA-150
d. Fakultas/Program studi	: Hukum/Ilmu Hukum
e. HP	: 081931603030
f. Alamat e-mail	: antonhendriks@yahoo.com
Anggota Peneliti (1)	
a. Nama Lengkap	: Dr. Go Lisanawati, S.H., M.Hum
b. NPK/ NIDN	: 204023/0723117702
c. Fakultas/Program studi	: Hukum/Ilmu Hukum
Lama Penelitian Keseluruhan	: 1 Tahun 6 bulan
Penelitian Tahun ke	: 1 dari 1 tahun
Biaya yang diusulkan	: Rp. 15.000.000,-

Surabaya, 1 September 2018

Menyetujui,

Ketua Lab.

Dr. Suhartati, S.H., M.Hum.
NPK: 203015

Dekan

Dr. Yoan N. Simanjuntak, S.H., M.Hum.
NPK: 196008

Ketua Peneliti

Anton Hendrik S., S.H., M.H.
NPK: 215020

RINGKASAN

Seiring berkembangnya zaman serta teknologi ternyata tidak hanya membawa dampak yang positif terhadap keberlangsungan hidup dimasyarakat, nyatanya disisi lain dampak negatif yang cukup besar pun dirasakan. Di era yang serba modern dan *online* ini memberikan metode dan modus baru bagi oknum-oknum pelaku kejahatan dalam menjalankan tindak pidananya. Salah satu contoh yang sering terjadi dimasyarakat adalah penipuan yang dilakukan secara *online* terkhususnya menggunakan kartu GSM yang disediakakan oleh berbagai jasa telekomunikasi di Indonesia. Terlalu mudahnya seseorang untuk mendapatkan kartu GSM dan mengaksesnya di*smartphone* masing-masing pribadi membawa implikasi penyalahgunaan bagi oknum-oknum yang ada. Sehingga pelaku tindak pidana yang dilakukan secara *online* tersebut dapat melakukan tanpa perlu menunjukan "muka"nya kepada korban (*faceless*). Akibatnya korban daripada tindak pidana tersebut mengalami kesusahan untuk mencaritahu atau mengungkap siapa yang menjadi pelaku tindak pidana sebenarnya. Berbagai celah yang masih terdapat dalam peraturan perundang-undangan kitapun semakin mempersulit pengungkapan identitas pelaku tindak pidana penipuan *online* tersebut.

Maka dari itu, peran dari pada penyedia jasa telekomunikasi di Indonesia terkhususnya di Surabaya menjadi titik penting dalam mencegah dan menanggulangi tindak penipuan *online* yang terjadi dimasyarakat. Berbagai prosedur standar yang dimiliki penyedia jasa telekomunikasi harus diatur sedemikian rupa agar dapat menjadi langkah awal mencegah disalahgunakannya kartu GSM yang menjadi produk mereka dimasyarakat. Kewajiban-kewajiban seperti harus meregistrasi kartu masing-masing pribadi yang sesuai dengan NIK dan KK asli haruslah menjadi tahapan pertama sebelum seseorang dapat mengakses atau menggunakan kartu GSM tersebut. Hal ini dibutuhkan untuk memberikkan "wajah" terhadap seluruh pengguna jasa telekomunikasi di Surabaya. Dengan diketahuinya "wajah" orang tersebut, apabila sewaktu-waktu disalahgunakan, berberkal dengan identitas tersebut penegak hukum dapat mencarinya dan menjatuhkan hukuman kepada oknum-oknum yang menyalahgunakannya.

DAFTAR ISI

BAB I

PENDAHULUAN

1. Latar Belakang

Trend belanja secara *online* sudah menjadi bagian dari perilaku manusia. Telah banyak aplikasi-aplikasi *cross platform*, dan *website* yang menyediakan jasa iklan jual beli *online*. Setiap kemudahan itu merupakan akselerator bagi perkembangan perekonomian, terlepas dari problem mekanisme perpajakan. Pelaku ekonomi juga bertambah banyak semakin hari karena kemudahan berbisnis via *online*. Berbisnis online ini juga didukung kemudahan dari pengiriman barang dengan adanya jasa transportasi *online* dan juga kurir. Kemudahan yang lainnya tentang mekanisme pembayaran yang diakomodasi oleh perbankan, seperti *internet banking*, dan *m-banking*.

Kemudahan-kemudahan tersebut diiringi juga tantangan atau ancaman, yaitu niat jahat dan perbuatan yang ingin mengambil keuntungan secara tercela. Anton menjelaskan bahwa untuk penipuan melalui transaksi jual beli *online*, politik hukumnya sudah berbeda. Modusnya, kecanggihannya, ancaman sanksi pidana yang sesuai konteks zaman ini, semuanya berbeda.[1]

Peluang kejahatan muncul disebabkan adanya titik lemah dari transaksi jual beli *online*, yaitu penjual dan pembeli tidak saling bertemu. Metodenya yang tidak menggunakan *cash and carry* membuat pelaku berpikir untuk memanfaatkan peluang untuk mendapatkan uang dengan cara menipu.[2] Pada transaksi jual beli *online* berlaku kebiasaan bahwa si pembeli harus melakukan pembayaran terlebih dahulu, apakah melalui transfer dana, kartu kredit atau rekening bersama. Dalam

[1] Anton Hendrik S. dan Andrian Julius, *Upaya Penanggulangan Tindak Pidana Penipuan Melalui Transaksi Jual Beli Online di Surabaya Dan Sekitarnya: Profil Modus Operandi Penipuan Melalui Transaksi Jual Beli Online yang Dilaporkan ke Reskrimsus Siber Polda Jatim*, Penelitian, LPPM Universitas Surabaya, 2016, h. 3
[2] *Ibid*., h. 1

hal ini, pembeli memiliki posisi tawar yang lemah, karena apabila pembeli tidak melakukan pembayaran terlebih dahulu, penjual tidak akan mengirimkan barang.

Kriminalisasi penipuan sudah ada sejak KUHP berlaku. Untuk penipuan melalui transaksi jual beli *online*, politik hukumnya sudah berbeda. Modusnya, kecanggihannya, ancaman sanksi pidana sesuai konteks zaman ini, semuanya berbeda. Dalam transaksi jual beli *online,* umumnya kesepakatan dilakukan tanpa bertemu secara fisik. Kemudian penjual/penyedia jasa memberitahukan rekening bank dan nama pemegang rekening ke konsumen, dan penjual/penyedia jasa menunggu sampai sejumlah uang yang disepakati ditransfer ke rekening mereka oleh konsumen. Setelah itu baru penjual/penyedia jasa melakukan *prestatie* sesuai yang disepakati. Penggunaan nama palsu, keadaan palsu, tipu muslihat, dan rangkaian kebohongan dilarang oleh KUHP, sebab dampaknya adalah membawa kerugian materiil bagi korban, yaitu korban dapat memberikan uang/barang sesuatu kepada pelaku karena terbujuk oleh rekayasanya.

Dalam KUHP perbuatan ini dilarang dan diancam sanksi di Pasal 378. Demikian isinya:

> "Barang siapa dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan memakai nama palsu atau martabat palsu, dengan tipu muslihat, ataupun rangkaian kebohongan, menggerakkan orang lain untuk menyerahkan barang sesuatu kepadanya, atau supaya memberi hutang maupun menghapuskan piutang diancam karena penipuan dengan pidana penjara paling lama empat tahun."

Sedangkan di dalam Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik (selanjutnya disebut UU ITE), aturan yang berkaitan dengan penanggulangan tindak pidana penipuan diatur dalam Pasal 28 ayat 1, yang isinya:

> "Setiap Orang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik."

Namun konstruksi pasal tersebut berbeda dengan konstruksi Pasal 378 KUHP. Di dalam Pasal 28 ayat 1 UU ITE tidak menggunakan istilah penipuan, melainkan

berita bohong.[3] Ancaman pidana untuk pelanggaran Pasal 28 ayat 1 UU ITE ini diatur dalam Pasal 45A ayat 1 Undang-undang No. 19 Tahun 2016 (untuk selanjutnya disebut dengan Perubahan UU ITE):

> "Setiap Orang yang dengan sengaja dan tanpa hak menyebarkan berita bohong dan menyesatkan yang mengakibatkan kerugian konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp 1.000. 000.000,00 (satu miliar rupiah)."

Peluang kejahatan didukung dengan bermacam-macam kegagalan sub-sistem dalam penyelenggaraan transaksi jual beli online. Temuan di penelitian terdahulu, dalam penyelenggaraan jasa telekomunikasi terdapat titik lemah yang digunakan oleh pelaku tindak pidana penipuan *online*, yaitu mudahnya dan murahnya mendapatkan kartu perdana GSM. Anton menjelaskan bahwa terdapat penyelenggara jasa telekomunikasi yang menawarkan harga dengan sangat murah untuk mendapatkan kartu perdana GSM, yaitu kisaran lima ribu rupiah. Para penyelenggara jasa telekomunikasi sebenarnya sudah melengkapi dengan fitur kewajiban mendaftarkan identitas untuk mengaktifkan kartu perdana, namun tidak ada mekanisme verifikasi kebenaran identitas yang didaftarkan untuk mengaktifkan kartu perdana. Sehingga, banyak sekali pengguna nomor GSM yang mendaftarkan identitas acak atau ngawur. Dengan adanya dua hal tersebut, yaitu kemudahan mendapatkan kartu perdana GSM dan tidak adanya mekanisme verifikasi identitas yang didaftarkan guna pengaktifan kartu, membuat pelaku tindak pidana penipuan terfasilitasi. Kemudahan ini yang membuat pelaku tindak pidana penipuan *online* dapat menggunakan nomor GSM seperti sekali pakai. Begitu pelaku mendapatkan korban dan keuntungan, nomor yang baru saja dipakai, dibuang dan ganti dengan nomor baru. Dalam praktik seperti inilah yang mengakibatkan penegak hukum kesulitan untuk melacak pelaku.

Seperti yang dijelaskan dalam penelitian sebelumnya, bahwa salah satu kendala pihak kepolisian yang lain adalah tidak adanya kewajiban bagi

[3] *Ibid*., h. 3

penyelenggara jasa telekomunikasi untuk membuka identitas pelaku tindak pidana penipuan *online*. Yang hal ini berbeda dengan perbankan yang terdapat pengaturan pengesampingan rahasia nasabah apabila penegakan hukum menghendakinya.

Oleh karena itu penyelenggara jasa telekomunikasi sebagai salah satu sub-sistem dalam penyelenggaraan kegiatan jual beli online harus bersinergi dan bekerjasama dengan penegak hukum dalam rangka pencegahan dan penanggulangan tindak pidana penipuan *online*.

2. Rumusan Masalah

1) Bagaimana prosedur standar penyelenggara jasa telekomunikasi di Surabaya terkait penyalahgunaan penggunaan jasa telekomunikasi sebagai sarana tindak pidana penipuan online?
2) Apa peran penyelenggara jasa telekomunikasi dalam upaya penanggulangan tindak pidana penipuan *online* di Surabaya?

3. Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut:

Tujuan akademik: Untuk menyelidiki dan menganalisis prosedur standar penyelenggara jasa telekomunikasi di Surabaya terkait penyalahgunaan penggunaan jasa telekomunikasi sebagai sarana tindak pidana penipuan online serta peran penyelenggara jasa telekomunikasi dalam penanggulangan tindak pidana penipuan online di Surabaya.

Tujuan Praktis: Sebagai bahan kajian penyusunan strategi kebijakan perihal penyelenggara jasa telekomunikasi sebagai sub-sistem dalam kegiatan transaksi jual-beli *online* untuk menanggulangi dan mencegah terjadinya penipuan melalui transaksi jual beli online dan sebagai panduan dalam proses penegakan hukum atas kasus tindak pidana penipuan *online*.

4. Manfaat Penelitian

Penelitian ini merupakan bagian dari gambaran besar dalam rangka melakukan upaya eliminasi sarana-sarana yang dapat digunakan pelaku untuk melaksanakan penipuan.

Manfaat penelitian ini adalah untuk mengukur dan mengevaluasi keterlibatan penyelenggara jasa telekomunikasi di Surabaya dalam penegakan hukum untuk kasus penipuan melalui transaksi jual beli online. Selain itu, melalui penelitian ini, ke depannya masyarakat dapat lebih mendapat edukasi dalam penggunaan layanan jasa telekomunikasi.

5. Urgensi Penelitian

Penelitian ini dapat memberikan manfaat keilmuan baik kepada kolega, dan mahasiswa, serta secara praktis bermanfaat bagi penegak hukum, dan pemerintah. Mengingat kerjasama antara penyelenggara jasa telekomunikasi dan kepolisian dapat mengakselerasi penanggulangan tindak pidana penipuan online yang tujuannya adalah melindungi masyarakat dari tindakan kejahatan terhadap harta kekayaan di tengah perkembangan teknologi.

BAB II

TINJAUAN PUSTAKA

II. 1. Kewajiban Penyelenggara Telekomunikasi

Indonesia merupakan salah satu negara yang memiliki jumlah operator terbanyak di dunia yakni 10 perusahaan. Hal ini bahkan membawa Indonesia menduduki posisi ke lima dalam negara pengguna *smartphone* terbanyak. Hasil ini menunjukkan bahwa penetrasi smartphone di Indonesia cukup deras, dan diperkirakan mencapai 100 juta pengguna.[4] Dengan jumlah pengguna yang sangat besar ini tentunya dapat menimbulkan berbagai peluang untuk melakukan tindak pidana. Salah satu tindak pidana yang sering kali terjadi adalah penipuan. Oleh sebab itu, penyelenggara jasa telekomunikasi yang berperan penting dalam keberlangsungannya harus memiliki peraturan-peraturan untuk mencegah ekses lebih jauh.

Dalam Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi (selanjutnya disebut dengan UU Telekomunikasi) tidak mengatur secara eksplisit mengenai kewajiban penyelenggara jasa telekomunikasi terhadap perlindungan pengguna. Namun hal tersebut tertuang dalam Pasal 23 Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 21 Tahun 2013 Tentang Penyelenggaraan Jasa Penyediaan Konten pada Jaringan Bergerak Seluler dan Jaringan Tetap Lokal Tanpa Kabel dengan Mobilitas Terbatas:

> "Pasal 23
> (1) Penyelenggara jaringan dan Penyelenggara Jasa Penyediaan Konten wajib melakukan upaya perlindungan Pengguna.
>
> (2) Perlindungan pengguna sebagaimana dimaksud pada ayat (1) meliputi perlindungan terhadap:
> a. gangguan *privacy*;
> b. penawaran yang mengganggu;

[4] "Indonesia Duduki Peringkat 5 Pengguna Smartphone Terbanyak Dunia", Kabar Bisnis, diakses dari http://www.kabarbisnis.com/read/2872380/indonesia-duduki-peringkat-5-pengguna-smartphone-terbanyak-dunia pada tanggal 16 Februari 2017 pukul 23.51

c. penipuan dan kejahatan melalui jaringan telekomunikasi; dan
d. tagihan pemakaian yang tidak wajar (*bill-shock*).

(3) Upaya perlindungan Pengguna sebagaimana dimaksud pada ayat (2) huruf a, huruf b, dan huruf c dapat dilakukan dengan cara meliputi:
a. menata ulang sistem registrasi pelanggan prabayar;
b. memasang system yang meminimalkan penyebaran pesan yang tidak semestinya; dan
c. membangun sistem tanggap cepat pengaduan/laporan konsumen"

Dalam peraturan tersebut disebutkan mengenai perlindungan pengguna hingga upaya perlindungan yang dapat dilaksanakan.

Lebih lanjut mengenai penyimpanan data pelanggan diatur dalam Pasal 17 Peraturan Menteri Nomor 12 Tahun 2016 bahwa:

"Pasal 17

(1) Penyelenggara Jasa Telekomunikasi wajib menyimpan data Pelanggan selama Pelanggan masih aktif berlangganan Jasa Telekomunikasi.
(2) Dalam hal Pelanggan sudah tidak aktif berlangganan Jasa Telekomunikasi, Penyelenggara Jasa Telekomunikasi wajib menyimpan data Pelanggan yang sudah tidak aktif dimaksud sesuai dengan ketentuan peraturan perundang-undangan.
(3) Penyelenggara Jasa Telekomunikasi wajib merahasiakan data dan/atau identitas Pelanggan kecuali ditentukan lain berdasarkan undang-undang.
(4) Dalam hal diperlukan, Penyelenggara Jasa Telekomunikasi wajib menyerahkan identitas Pelanggan sebagaimana dimaksud dalam Pasal 3 atas permintaan:
    a. Jaksa Agung dan/atau Kepala Kepolisian Republik Indonesia untuk proses peradilan tindak pidana tertentu;
    b. Penyidik untuk proses peradilan tindak pidana tertentu lainnya sesuai dengan ketentuan peraturan perundang-undangan;
    c. Menteri untuk keperluan kebijakan di bidang telekomunikasi;
    d. Instansi pemerintah yang menyelenggarakan urusan di bidang kependudukan untuk keperluan Validasi; dan/atau
    e. Instansi pemerintah lain sesuai ketentuan peraturan perundang-undangan.
(5) Penyelenggara Jasa Telekomunikasi wajib memiliki sertifikasi paling rendah ISO 27001 untuk keamanan informasi dalam pengelolaan data Pelanggan paling lambat 18 (delapan belas) bulan sejak Peraturan Menteri ini mulai berlaku."

Penjelasan Umum Peraturan Pemerintah Republik Indonesia Nomor 52 Tahun 2000 Tentang Penyelenggaraan Komunikasi bahwa:

> "Penyelenggaraan jasa telekomunikasi diwajibkan untuk pertama, menyediakan fasilitas telekomunikasi yang menjamin adanya kualitas pelayanan jasa telekomunikasi yang baik. Kedua, penyelenggara jasa telekomunikasi dituntut untuk tidak bersikap diskriminatif dalam memberikan pelayanan kepada pengguna jasa telekomunikasi. Ketiga, penyelenggara jasa telekomunikasi diwajibkan untuk melakukan pencatatan/ perekaman pemakaian jasa telekomunikasi, serta wajib menyimpan catatan/rekaman dimaksud sekurang-kurangnya selama 3 (tiga) bulan."

Pasal 41 dan Pasal 42 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi:

> "Pasal 41
> Dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi atas permintaan pengguna jasa telekomunikasi, penyelenggara jasa telekomunikasi wajib melakukan perekaman pemakaian fasilitas telekomunikasi yang digunakan oleh pengguna jasa telekomunikasi dan dapat melakukan perekaman informasi sesuai dengan peraturan perundang-undangan yang berlaku.
>
> Pasal 42
> (1) Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima, oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.
> (2) Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atas:
> a. permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu;
> b. permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-undang yang berlaku.
> (3) Ketentuan mengenai tata cara permintaan dan pemberian rekaman informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah."

II. 2 Registrasi Data Pengguna Nomor MSISDN

Pasal 4 Peraturan Menteri Nomor 12 Tahun 2016 yakni:

"(1) Registrasi Pelanggan Prabayar dilakukan melalui:

a. gerai milik Penyelenggara Jasa Telekomunikasi atau gerai milik Mitra; atau
b. Registrasi sendiri.

(2) Registrasi sendiri sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui:
a. layanan pesan singkat atau Pusat Kontak Layanan Penyelenggara Jasa Telekomunikasi yang diakses melalui Nomor MSISDN yang akan didaftarkan; atau
b. laman situs milik Penyelenggara Jasa Telekomunikasi dengan menerapkan metode pembuktian kebenaran Nomor MSISDN yang didaftarkan."

Lebih lanjut di atur pula dalam Pasal 5, 6 dan 7 Peraturan Menteri Nomor 12 Tahun 2016 mengenai tata cara registrasi pelanggan prabayar yakni:

"Pasal 5
Registrasi melalui gerai sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a dilakukan dengan tahapan sebagai berikut:
a. registrasi dilakukan oleh petugas gerai yang ditunjuk oleh Penyelenggara Jasa Telekomunikasi atau Mitra;
b. petugas gerai melakukan Verifikasi terhadap identitas calon Pelanggan Prabayar sebagaimana dimaksud dalam Pasal 3;
c. untuk proses registrasi menggunakan NIK:
   1. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi; dan
   2. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil.
d. untuk proses Registrasi yang menggunakan Paspor, KITAP, atau KITAS, petugas gerai mencatat data calon Pelanggan Prabayar paling sedikit:
   1. nama;
   2. nomor identitas dari Paspor, KITAP, atau KITAS;
   3. kewarganegaraan; dan
   4. tempat dan tanggal lahir.

Pasal 6
Registrasi sendiri melalui layanan pesan singkat atau Pusat Kontak Layanan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a dilakukan oleh calon Pelanggan Prabayar dengan tahapan sebagai berikut:
a. calon Pelanggan Prabayar mengirimkan layanan pesan singkat atau menghubungi Pusat Kontak Layanan yang diakses melalui Nomor MSISDN yang akan didaftarkan dengan mengirimkan/menyampaikan data berupa:
   1. NIK; dan
   2. nama ibu kandung atau nomor Kartu Keluarga.

b. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi;
c. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil; dan
d. dalam hal data yang dimasukkan tidak tervalidasi, calon Pelanggan Prabayar diberikan kesempatan untuk melakukan Registrasi kembali paling banyak 5 (lima) kali.

Pasal 7
Registrasi sendiri melalui laman situs Penyelenggara Jasa Telekomunikasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b dilakukan oleh calon Pelanggan Prabayar dengan tahapan sebagai berikut:
a. calon Pelanggan Prabayar mengisi dan mengirimkan Nomor MSISDN yang akan didaftarkan pada laman situs milik Penyelenggara Jasa Telekomunikasi;
b. setelah pengiriman Nomor MSISDN berhasil, Penyelenggara Jasa Telekomunikasi mengirimkan kode otorisasi yang dapat berupa One-Time Password ke Nomor MSISDN calon Pelanggan Prabayar yang akan didaftarkan;
c. setelah menerima kode otorisasi sebagaimana dimaksud pada huruf b, calon Pelanggan Prabayar mengirimkan kembali:
    1. kode otorisasi;
    2. NIK; dan
    3. nama ibu kandung atau nomor Kartu Keluarga;
d. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi;
e. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil; dan
f. dalam hal data yang dimasukkan tidak tervalidasi, calon Pelanggan Prabayar diberikan kesempatan untuk melakukan Registrasi kembali paling banyak 5 (lima) kali."

II. 3 Tugas Pokok dan Fungsi Kepolisian Negara Republik Indonesia

Kepolisian sebagai salah satu aparat penegak hukum di Indonesia tentunya memegang peranan penting dalam mencegah dan mengawasi jalannya bisnis secara *online*. Kepolisian tidak dapat bekerja tanpa adanya peran serta dari masyarakat, khususnya pihak-pihak yang terlibat dalam penyelenggaraan bisnis *online*, yaitu perbankan, dan penyelenggara jasa telekomunikasi. Kepolisian Negara Republik Indonesia, yang selanjutnya disebut dengan POLRI, sesuai pengertian pasal 1 huruf a Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik

Indonesia (UU POLRI) dijelaskan bahwa; “Kepolisian adalah segala hal-ihwal yang berkaitan dengan fungsi dan lembaga polisi sesuai dengan peraturan perundang-undangan.” Sebagai salah satu dari beberapa lembaga penegak hukum yang ada di Indonesia, POLRI pada hakekatnya memiliki tiga tugas pokok, sesuai Pasal 13 UU POLRI, yaitu:

a. Memelihara keamanan dan ketertiban masyarakat;
b. Menegakkan hukum; dan
c. Memberikan perlindungan, pengayoman, dan pelayanan kepada masyarakat.

Penyidikan dalam UU ITE diatur di dalam Bab X, di Pasal 42 dinyatakan bahwa penyidikan dilakukan berdasarkan Hukum Acara Pidana dan ketentuan UU ITE. Yang dimaksud dengan Hukum Acara Pidana, adalah hukum acara pidana secara umum yang diatur dalam Undang-undang No. 8 Tahun 1981 Tentang Hukum Acara Pidana (selanjutnya disebut KUHAP). Dalam UU ITE tidak diatur secara khusus mengenai penyelidikan, hanya penyidikan. Sehingga proses penyelidikan mengikuti aturan KUHAP sebagai *lex generalis* hukum acara pidana.

Penyelidik adalah pejabat polisi negara Republik Indonesia yang diberi wewenang atributif untuk melakukan penyelidikan. Penyelidikan adalah serangkaian tindakan penyelidik untuk mencari dan menemukan suatu peristiwa yang diduga sebagai tindak pidana guna menentukan dapat atau tidaknya dilakukan penyidikan menurut cara yang diatur dalam undang-undang. Penyidik adalah pejabat polisi negara Republik Indonesia atau pejabat pegawainegeri sipil tertentu yang diberi wewenang khusus oleh undang-undang untukmelakukan penyidikan. Penyidikan adalah serangkaian tindakan penyidik dalam hal dan menurut carayang diatur dalam undang-undang untuk mencari serta mengumpulkan buktiyang dengan bukti itu membuat terang tentang tindak pidana yang terjadi danguna menemukan tersangkanya.

Dalam UU ITE disebutkan bahwa penyidik bisa dari pejabat POLRI atau pejabat pegawai negeri sipil (PPNS) yang bertanggung jawab di bidang teknologi

informasi dan transaksi elektronik. Sedangkan fungsi penyelidik hanya dapat dilakukan oleh pejabat POLRI yang diberi wewenang secara atributif.

Mengingat kekhususan tindak pidana yang dilakukan menggunakan teknologi informasi memerlukan kompetensi yang khusus. Sehingga dalam internal POLRI wewenang penyelidikan dan penyidikan didistribusi secara khusus ke reserse kriminal khusus, dalam hal ini adalah reserse criminal khusus siber. Ketiga tugas pokok tersebut kemudian dijabarkan lebih lanjut ke dalam berbagai tugas dan wewenang sesuai pengaturan Pasal 14 dan Pasal 15. Namun dalam hal terkait penegakan atas tindak pidana khususnya di bidang *cyber*, dalam UU disebutkan secara eksplisit bahwa POLRI berfungsi melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa lainnya dan di saat yang bersamaan berhak melakukan penyelidikan dan penyidikan terhadap semua tindak pidana sesuai dengan hukum acara pidana dan peraturan perundang-undangan lainnya yang berlaku.

Terkait dengan isu yang diangkat dalam penelitian ini, maka tentu yang dimaksud dengan kepolisian khusus adalah Direktorat Reserse Kriminal Khusus Subdit *Cyber Crime* yang bertugas untuk menangani kejahatan di bidang *cyber* atau yang menurut dokumen kongres PBB tentang *The Prevention of Crime and The Treatment of Offlenderes di Havana, Cuba* pada tahun 1999 dan di Wina, Austria tahun 2000; "*Cyber crime in a broader sense are computer related crime: any illegal behaviour committed by means on relation to, a computer system offering or system or network, including such crime as illegal possession in, offering or distributing information by means of computer system or network*" atau singkatnya kejahatan terkait komputer. Sementara Undang-undang lain yang perlu dijadikan rujukan tentu adalah Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik beserta dengan perubahannya yaitu Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

BAB III

METODE PENELITIAN

Penelitian hukum yang dilaksanakan merupakan kesinambungan dari upaya untuk memperdalam keahlian di bidang hukum pidana siber, memperkaya literatur di Indonesia mengenai implementasi UU ITE dan perubahannya, dan memberi saran akademis maupun praktis terhadap penegakan hukum tindak pidana penipuan melalui teknologi informasi komunikasi. Penelitian ini juga dilakukan dalam rangka memperkaya wawasan kepada peserta didik dalam mata kuliah Kejahatan Siber.

Sesuai dengan Rencana Induk Penelitian (RIP) yang telah dirumuskan oleh UBAYA, penelitian ini dirancang dengan memberikan perumusan perencanaan penelitian menggunakan pengkajian normatif dan empirik atas pengembangan ilmu pengetahuan, produktifitas bisnis, kesejahteraan manusia, mutu lingkungan, serta pembangunan nasional. Terkait dengan RIP UBAYA, penelitian ini menggunakan klaster *Healthy Living*, dalam hal ini terkait dengan kelembagaan pemerintah dan produk hukumnya, dengan dikaitkan pada profil modus penipuan melalui teknologi informasi komunikasi, pelaksanaan penegakan hukum dan subsistem terkait identitas dan rekening pelaku. Hasil penelitian ini akan memberikan input baik pada penegak hukum maupun pemerintah dalam pencegahan dan penanggulangan tindak pidana penipuan melalui teknologi informasi yang semakin berkembang dan meresahkan masyarakat.

Metodologi penelitian yang dipilih dalam penelitian ini adalah menggunakan metode penelitian hukum yuridis normatif yang ditunjang dengan metode penelitian yuridis empiris.

Desain Penelitian:

Penelitian hukum ini merupakan penelitian kualitatif, yang didasarkan pada sebuah pengembangan cara berpikir induksi, yang dilakukan melalui observasi (pengamatan), kemudian dilakukan hermeunetik untuk kemudian dihasilkan suatu teori. Metode penelitian yang digunakan adalah metode penelitian hukum yuridis normatif dilengkapi dengan metode penelitian hukum yuridis empiris. Kegiatan yang juga akan dilakukan adalah pengamatan, wawancara, dan analisis dokumen.

Metode Penelitian Hukum Yuridis Normatif

Penelitian ini dilakukan melalui studi pustaka atas peraturan perundang-undangan yang terkait tindak pidana penipuan melalui teknologi informasi beserta doktrin-doktrin hukum yang terkait.

a. Metode Pendekatan

Metode pendekatan yang digunakan dalam penelitian ini adalah melalui pendekatan peraturan perundang-undangan (*statute approach*), dan pendekatan konseptual (*conceptual approach*). Kedua pendekatan tersebut digunakan untuk menganalisis dan memberi pemecahan masalah (*problem solving*).

b. Bahan Hukum

Bahan hukum yang digunakan dalam penelitian ini adalah:

- Bahan hukum primer, yang meliputi Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Undang-undang No. 19 Tahun 2016 Tentang Perubahan Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik, Kitab Undang-undang Hukum Pidana, Undang-undang Tentang 36 Tahun 1999 Tentang Telekomunikasi, Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016 Tentang Registrasi Pelanggan Jasa Telekomunikasi,

- Bahan hukum sekunder, yang meliputi doktrin-doktrin yang ditemukan dalam berbagai literatur, dan asas-asas hukum yang terkait dengan permasalahan tindak pidana penipuan melalui informasi teknologi.

c. Langkah Analisis

Pengumpulan bahan hukum dilakukan melalui penelusuran pustaka yang diawali dengan inventarisasi, klasifikasi, dan sistemasi bahan hukum. Untuk menganalisis, dilakukan deskripsi analisis atas bahan-bahan hukum yang diawali dengan menelaah bahan-bahan hukum primer dengan menggunakan metode deduksi.

Metode Penelitian Hukum Yuridis Empiris

Pengambilan data di lapangan juga dilakukan melalui observasi, analisis dokumen, dan wawancara narasumber. Hasil data lapangan akan di analisis bersama dengan hasil deduksi bahan hukum.

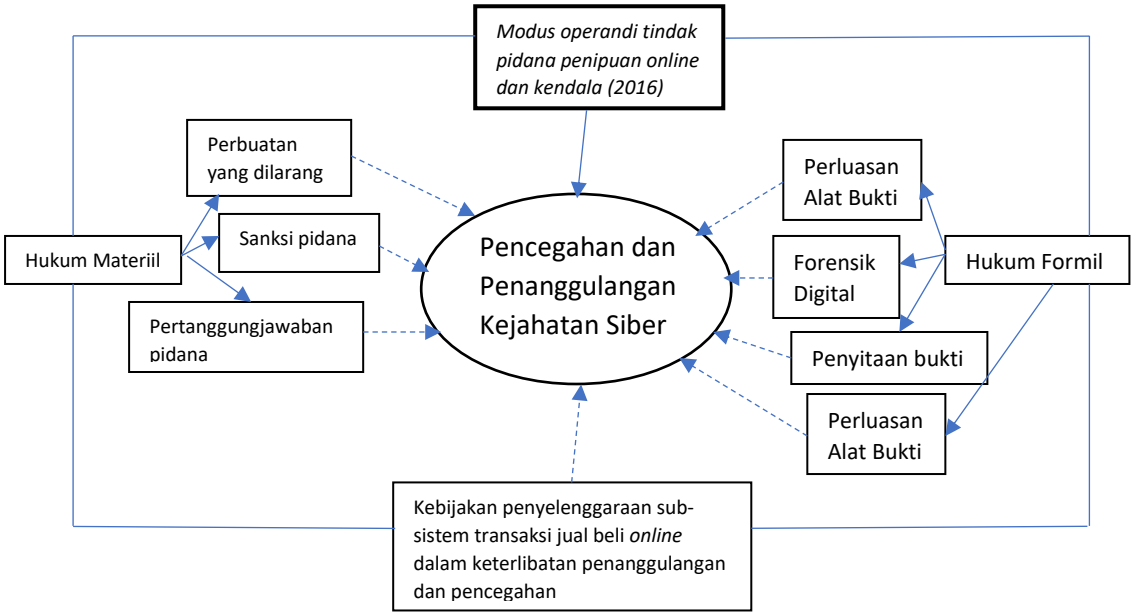
Untuk memperkuat analisis, perlu diperoleh data hasil survei dan wawancara terhadap informan kunci yang berkompeten, antara lain Kepolisian Resort Kota Besar Surabaya, dan Penyelenggara Jasa Telekomunikasi.

Penelitian tentang peran penyelenggara jasa telekomunikasi dalam upaya pencegahan dan penanggulangan tindak pidana penipuan online di kota Surabaya ini sangat penting untuk dilakukan mengingat masih maraknya tindak pidana tersebut. Kajian akademis praktis perlu dilakukan untuk memberi masukan untuk pencegahan dan penanggulangannya, sehingga solusi yang ditawarkan nantinya lebih aplikatif.

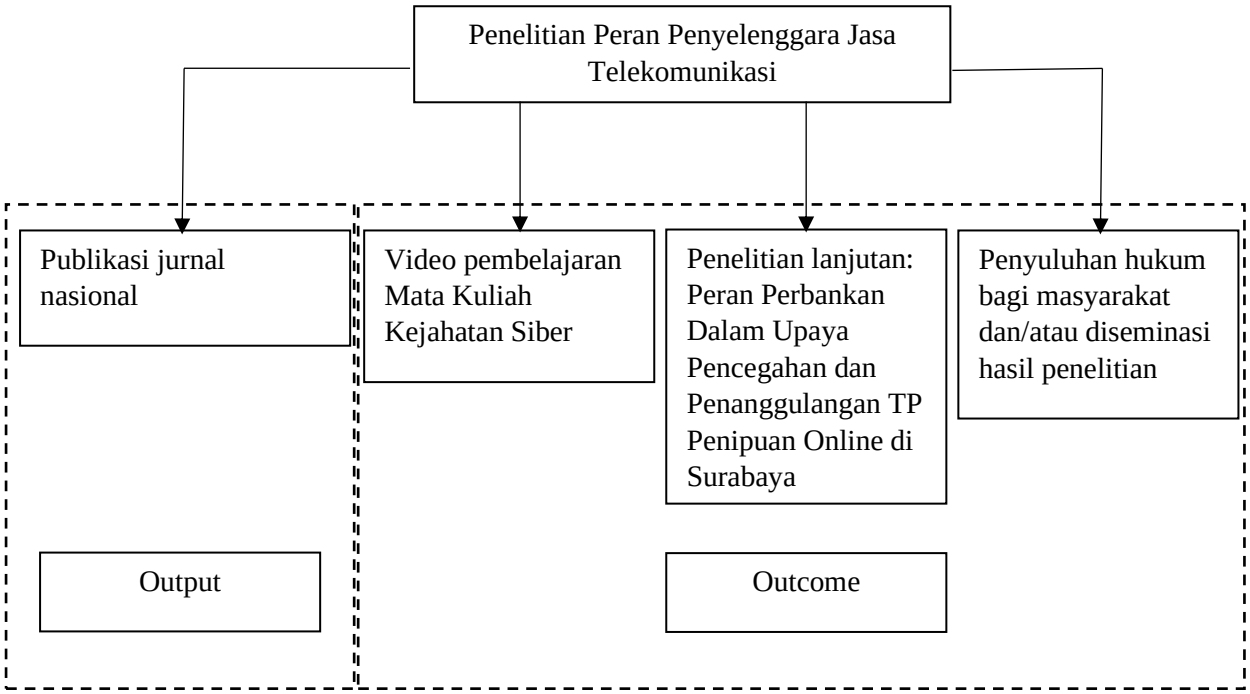
Future Research

Terkait dengan hasil penelitian ini, diharapkan dapat dikembangkan penelitian selanjutnya yang masih dalam kerangka peran sub-sistem yang terkait kegiatan transaksi jual-beli online dalam upaya pencegahan dan penanggulangan tindak pidana penipuan *online*. Mengingat perbuatan demikian dilarang dan diancam pidana untuk melindungi kepentingan masyarakat dari kejahatan terhadap harta kekayaan.

Adapun bagan alir penelitian sebagai berikut:



Melalui flowchart berikut ini dijelaskan mengenai *output* dan *outcome* dari penelitian yang akan dilaksanakan:



BAB IV

HASIL DAN PEMBAHASAN

IV.1. Prosedur Standar Penyelenggara Jasa Telekomunikasi di Surabaya Terkait Penyalahgunaan Jasa Telekomunikasi Sebagai Sarana Tindak Pidana Penipuan *Online*

Berbelanja secara *online* melalui cara *browsing website* memberikan kenyamanan bagi kebanyakan penggunanya. Pembeli tidak perlu lagi repot-repot pergi ke pusat perbelanjaan dan berkeliling, cukup beberapa klik, kemudian menghubungi penjual, transfer pembayaran, dan barang akan muncul di depan pintu kita diantar kurir/jasa pengiriman. Umumnya, setelah korban melihat informasi berupa iklan dalam *website*, mereka akan menghubungi penjual (yang adalah pelaku) secara personal menggunakan kontak yang diberikan penjual di *website* tersebut.[5]

Sebagaimana telah dipaparkan dalam penelitian sebelumnya, bahwa sarana yang kerap digunakan pelaku adalah *website*, *email*, telepon dan SMS untuk menjangkau korban. Melalui rangkaian *social engineering*, rangkaian kegiatan tersebut berujung pada korban mentransferkan sejumlah uang ke rekening yang dimaksud pelaku tanpa adanya kontra-prestasi. Jasa telekomunikasi merupakan kunci untuk mendapatkan akses ke internet juga.

Di era siber sekarang ini, masyarakat penghuni dunia siber sangat menghendaki jaminan keamanan dan privasi. Perkembangan teknologi berbanding lurus dengan perkembangan jaminan keamanan dan privasi pengguna internet. Keamanan dan privasi melindungi semua orang, tak terkecuali orang yang memiliki niat jahat.[6] Dalam praktik penyelidikan dan penyidikan, lebih mudah untuk mengungkap kasus penipuan yang pelaku dan korbannya bertemu muka dengan muka. Karena hal tersebut jelas mengindikasikan bahwa pelakunya benar-benar ada, daripada yang terjadi pada kasus penipuan *online* yang pelakunya bisa jadi

[5] Anton Hendrik S. dan Andrian Julius, *Op.Cit.*, hal. 23-24
[6] *Ibid*., hal. 27

fiktif keberadaannya. Peneliti berpendapat bahwa fenomena ini dapat dikategorikan sebagai *faceless crime*, yang merupakan satu hal yang menguntungkan pelaku kejahatan karena wajahnya tidak pernah diketahui sehingga sulit untuk menangkap mereka agar memertanggungjawabkan secara hukum.[7]

Sebenarnya tidak ada prosedur standar khusus mengenai penanganan penyalahgunaan penggunaan jasa telekomunikasi yang digunakan untuk menjalankan tindak pidana penipuan. Meksipun demikian, penyelenggara jasa telekomunikasi bersedia bekerja sama dengan penegak hukum, berdasarkan Peraturan Menteri Nomor 12 Tahun 2016. Namun memang kesepakatan internal mereka yang cukup ketat juga menimbulkan kendala dalam proses penyidikan kasus tindak pidana penipuan *online*.

Membuka identitas dari pengguna GSM yang adalah konsumen dari penyedia jasa telekomunikasi juga masih menjadi kendala dal am penyidikan. Jika dalam perbankan rahasia nasabah dapat dikesampingkan untuk kepentingan penegakan hukum oleh UU Perbankan dan PBI 2/19/2000, masih belum ada peraturan yang mewajibkan penyedia jasa telekomunikasi untuk membuka data konsumen mereka untuk kepentingan penegakan hukum. Seringnya penyidik dipersulit, karena penyedia jasa telekomunikasi tidak mau kehilangan kepercayaan konsumen terhadap layanan mereka, yang dalam hal ini adalah privasi.[8] Meskipun demikian, telah terjadi kesepahaman dalam internal penyelenggara jasa telekomunikasi bahwa kerjasama dalam rangka penegakan hukum terbuka lebar asalkan sesuai dengan prosedur.

Pada temuan penelitian sebelumnya, dinyatakan bahwa kendala yang dialami penyidik dalam mengungkap tindak pidana penipuan *online* adalah validitas identitas pelaku.[9] Pelaku mendapatkan peluang dari kurangnya regulasi penggunaan kartu GSM prabayar dan mengeksploitasinya untuk melakukan kejahatan. Murah dan mudah didapatnya kartu GSM prabayar tersebut menjadi

[7] *Ibid*., hal. 20
[8] *Ibid*., hal. 27
[9] *Ibid*.

sarana akselerasi tindak pidana penipuan *online*. Pelaku menggunakan kartu GSM prabayar sebagai bagian dari upaya *social engineering*, dan itu menjadi salah satu bagian terpenting dalam melancarkan tindak pidana penipuan *online*. Sesudah berhasil mendapatkan keuntungan dari korban, pelaku akan membuang kartu GSM prabayar dan membeli lagi yang baru. Hal itu dilaksanakan agar tidak tertangkap oleh penegak hukum.

Oleh karena itu, perlu diadakan pengaturan yang dapat mengeliminir kesempatan pelaku melakukan eksploitasi sarana yang dapat dilakukan untuk melakukan kejahatan. Langkah awal sebagai tersebut kemudian dituangkan dalam prosedur standar penyelenggara jasa telekomunikasi yakni melakukan registrasi terhadap seluruh kartu perdana yang diedarkan sebagai mana telah diatur dalam Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016 Tentang Registrasi Pelanggan Jasa Telekomunikasi (selanjutnya disebut Peraturan Menteri Nomor 12 Tahun 2016). Registrasi tersebut dapat dilakukan dengan beberapa cara sesuai dengan Pasal 4 Peraturan Menteri Nomor 12 Tahun 2016 yakni:

> "(1) Registrasi Pelanggan Prabayar dilakukan melalui:
>
> a. gerai milik Penyelenggara Jasa Telekomunikasi atau gerai milik Mitra; atau
> b. Registrasi sendiri.
>
> (2) Registrasi sendiri sebagaimana dimaksud pada ayat (1) huruf b dilakukan melalui:
>
> a. layanan pesan singkat atau Pusat Kontak Layanan Penyelenggara Jasa Telekomunikasi yang diakses melalui Nomor MSISDN yang akan didaftarkan; atau
> b. laman situs milik Penyelenggara Jasa Telekomunikasi dengan menerapkan metode pembuktian kebenaran Nomor MSISDN yang didaftarkan."

Proses registrasi yang harus dilakukan pengguna jasa telekomunikasi adalah menginputkan Nomor Induk Kependudukan (NIK) dan Nomor Kartu Keluarga (Nomor KK) ke dalam sistem penyelenggara telekomunikasi. Lebih lanjut di atur pula dalam Pasal 5, 6 dan 7 Peraturan Menteri Nomor 12 Tahun 2016 mengenai tata cara registrasi pelanggan prabayar yakni:

“Pasal 5

Registrasi melalui gerai sebagaimana dimaksud dalam Pasal 4 ayat (1) huruf a dilakukan dengan tahapan sebagai berikut:

a. registrasi dilakukan oleh petugas gerai yang ditunjuk oleh Penyelenggara Jasa Telekomunikasi atau Mitra;
b. petugas gerai melakukan Verifikasi terhadap identitas calon Pelanggan Prabayar sebagaimana dimaksud dalam Pasal 3;
c. untuk proses registrasi menggunakan NIK:
    1. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi; dan
    2. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil.
d. untuk proses Registrasi yang menggunakan Paspor, KITAP, atau KITAS, petugas gerai mencatat data calon Pelanggan Prabayar paling sedikit:
    1. nama;
    2. nomor identitas dari Paspor, KITAP, atau KITAS;
    3. kewarganegaraan; dan
    4. tempat dan tanggal lahir.

Pasal 6

Registrasi sendiri melalui layanan pesan singkat atau Pusat Kontak Layanan sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf a dilakukan oleh calon Pelanggan Prabayar dengan tahapan sebagai berikut:

a. calon Pelanggan Prabayar mengirimkan layanan pesan singkat atau menghubungi Pusat Kontak Layanan yang diakses melalui Nomor MSISDN yang akan didaftarkan dengan mengirimkan/menyampaikan data berupa:
    1. NIK; dan
    2. nama ibu kandung atau nomor Kartu Keluarga.
b. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi;
c. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil; dan
d. dalam hal data yang dimasukkan tidak tervalidasi, calon Pelanggan Prabayar diberikan kesempatan untuk melakukan Registrasi kembali paling banyak 5 (lima) kali.

Pasal 7

Registrasi sendiri melalui laman situs Penyelenggara Jasa Telekomunikasi sebagaimana dimaksud dalam Pasal 4 ayat (2) huruf b dilakukan oleh calon Pelanggan Prabayar dengan tahapan sebagai berikut:

a. calon Pelanggan Prabayar mengisi dan mengirimkan Nomor MSISDN yang akan didaftarkan pada laman situs milik Penyelenggara Jasa Telekomunikasi;

b. setelah pengiriman Nomor MSISDN berhasil, Penyelenggara Jasa Telekomunikasi mengirimkan kode otorisasi yang dapat berupa One-Time Password ke Nomor MSISDN calon Pelanggan Prabayar yang akan didaftarkan;
c. setelah menerima kode otorisasi sebagaimana dimaksud pada huruf b, calon Pelanggan Prabayar mengirimkan kembali:
   1. kode otorisasi;
   2. NIK; dan
   3. nama ibu kandung atau nomor Kartu Keluarga;
d. setelah menerima data dari calon Pelanggan Prabayar, Penyelenggara Jasa Telekomunikasi melakukan Validasi;
e. dalam hal data yang dimasukkan oleh calon Pelanggan Prabayar tervalidasi, proses Registrasi dinyatakan berhasil; dan
f. dalam hal data yang dimasukkan tidak tervalidasi, calon Pelanggan Prabayar diberikan kesempatan untuk melakukan Registrasi kembali paling banyak 5 (lima) kali."

Dalam Pasal 5, 6 dan 7 tersebut menunjukkan terdapat tiga cara registrasi, yaitu dengan cara mengirimkan SMS, melalui petugas gerai, dan melalui laman situs penyelenggara jasa telekomunikasi. Opsi ini memudahkan pengguna sekaligus meniadakan alasan kesulitan melakukan registrasi.

Kewajiban registrasi ini merupakan upaya untuk memberi 'wajah' pada setiap pengguna jasa telekomunikasi. Yang sebelumnya, apabila terjadi kejahatan, dalam proses penyidikan ketika penyidik membuka data pengguna jasa telekomunikasi, ditemukan bahwa identitas yang terdaftar adalah palsu. Ketika didatangi di alamat yang terdaftar, penyidik menemukan jalan buntu dan tidak mendapatkan pelaku kejahatannya.

Langkah selanjutnya mengenai upaya pencegahan penyalahgunaan nomor pelanggan prabayar nyatanya telah diatur pula dalam Pasal 11 Peraturan Menteri Nomor 12 Tahun 2016 yakni bahwa calon pelanggan prabayar hanya dapat meregistrasi sendiri maksimal 3 nomor *Mobile Subscriber Integrated Services Digital Network* (selanjutnya disebut Nomor MSISDN) atau nomor pelanggan untuk setiap NIK pada setiap penyelenggara jasa telekomuniasi, apabila nomor MSISDN kebutuhannya lebih dari 3 maka hanya dapat diregistrasi melalui gerai milik penyelenggara jasa telekomunikasi atau gerai milik mitra, selain itu penyelenggara jasa telekomunikasi juga wajib menonaktifkan nomor MSISDN atau

nomor pelanggan apabila terbukti menggunakan identitas palsu, tidak benar, milik orang lain tanpa hak atau tanpa izin orang bersangkutan dan yang terbukti disalahgunakan.

Lebih lanjut mengenai penyimpanan data pelanggan diatur dalam Pasal 17 Peraturan Menteri Nomor 12 Tahun 2016 bahwa:

"Pasal 17

(1) Penyelenggara Jasa Telekomunikasi wajib menyimpan data Pelanggan selama Pelanggan masih aktif berlangganan Jasa Telekomunikasi.
(2) Dalam hal Pelanggan sudah tidak aktif berlangganan Jasa Telekomunikasi, Penyelenggara Jasa Telekomunikasi wajib menyimpan data Pelanggan yang sudah tidak aktif dimaksud sesuai dengan ketentuan peraturan perundang-undangan.
(3) Penyelenggara Jasa Telekomunikasi wajib merahasiakan data dan/atau identitas Pelanggan kecuali ditentukan lain berdasarkan undang-undang.
(4) Dalam hal diperlukan, Penyelenggara Jasa Telekomunikasi wajib menyerahkan identitas Pelanggan sebagaimana dimaksud dalam Pasal 3 atas permintaan:
    a. Jaksa Agung dan/atau Kepala Kepolisian Republik Indonesia untuk proses peradilan tindak pidana tertentu;
    b. Penyidik untuk proses peradilan tindak pidana tertentu lainnya sesuai dengan ketentuan peraturan perundang-undangan;
    c. Menteri untuk keperluan kebijakan di bidang telekomunikasi;
    d. Instansi pemerintah yang menyelenggarakan urusan di bidang kependudukan untuk keperluan Validasi; dan/atau
    e. Instansi pemerintah lain sesuai ketentuan peraturan perundang-undangan.
(5) Penyelenggara Jasa Telekomunikasi wajib memiliki sertifikasi paling rendah ISO 27001 untuk keamanan informasi dalam pengelolaan data Pelanggan paling lambat 18 (delapan belas) bulan sejak Peraturan Menteri ini mulai berlaku."

Upaya memberantas dan menanggulangi kejahatan, selain menghukum pelaku agar tercapai *special* dan *general deterrence effect*, adalah mengeliminasi sarana-sarana maupun kesempatan untuk melakukan kejahatan dan/atau upaya menyembunyikan diri agar tidak tertangkap. Memberi 'wajah' dengan cara mewajibkan pengguna jasa telekomunikasi untuk melakukan registrasi merupakan salah satu upaya untuk menghilangkan sarana kejahatan dan/atau menyembunyikan diri agar tidak tertangkap. Apabila ada pelaku tindak pidana penipuan yang

membangun rangkaian kata bohong atau tipu muslihatnya atau menjalankan *sosial engineering* menggunakan komunikasi berbasis Nomor MSISDN, paling tidak identitas pelaku sudah bisa didapat dan itu valid.

Meskipun pengguna melakukan registrasi dengan memasukkan NIK dan Nomor Kartu Keluarga yang kemudian divalidasi, penyelenggara jasa telekomunikasi tidak menyimpan data kependudukan masyarakat Indonesia. Dikatakan oleh Sabirin Mochtar, Tb. Apriza Mulqi dan M. Yusuf Firdaus berturut-turut sebagai Plt. Direktur Pengendalian Dirjen PPI, Kasubbag Tata Usaha, Setditjen PPI, dan ADC Dirjen PPI Kementerian Komunikasi dan Informatika, bahwa dalam proses registrasi sewaktu pengguna menginputkan NIK dan Nomor Kartu Keluarga, proses validasinya adalah *bypassing* ke dalam sistem elektronik milik Dinas Kependudukan dan Pencatatan Sipil. Senada juga disampaikan oleh Sutrisman. Proses validasinya memang *bypassing*, namun karena ada proses penginputan, data NIK dan Nomor Kartu Keluarga yang diinputkan juga akhirnya masuk ke dalam sistem penyelenggara jasa telekomunikasi. Implikasinya adalah penyelenggara jasa telekomunikasi harus menjaga integritas penyelenggaraan dan perlindungan data pengguna, dan penegak hukum dapat meminta data pelaku tindak pidana penipuan *online* langsung lengkap di pintu penyelenggara jasa telekomunikasi tanpa harus memintanya pada Dinas Kependudukan dan Pencatatan Sipil.

Dengan adanya proses registrasi yang telah dijelaskan, bukan berarti tindakan preventif sudah cukup untuk menekan agar jasa telekomunikasi tidak dijadikan sarana tindak pidana penipuan *online*. Pada dasarnya NIK dan Nomor KK sudah tersebar di mana-mana. Ketika nasabah bank mengajukan pinjaman atau kredit, kartu kredit, atau juga mendaftar sekolah atau kuliah, semua menggunakan KK yang juga terdapat NIK di dalamnya. Orang yang memiliki niat jahat bisa saja melakukan registrasi Nomor MSISDN dengan menggunakan NIK dan nomor KK orang lain, kemudian melaksanakan tindak pidana penipuan *online*.

IV.2. Peran Penyelenggara Jasa Telekomunikasi Dalam Upaya Penanggulangan Tindak Pidana Penipuan *Online* di Surabaya

Peran penyelenggara jasa telekomunikasi dapat dibagi menjadi peran dalam upaya preventif dan peran dalam upaya represif. Peran preventif menekankan pada upaya-upaya mengeliminasi jasa telekomunikasi dijadikan sebagai sarana kejahatan atau dalam rangka *social engineering*[10] untuk melaksanakan tindak pidana penipuan *online*. Sedangkan peran represif menekankan pada upaya penanggulangan pasca-terjadinya tindak pidana. Menekankan bagaimana kerjasama penyelenggara jasa telekomunikasi dalam proses penyelidikan, penyidikan, dan peradilan.

Salah satu bentuk peran penyelenggara jasa telekomunikasi sebagaimana diamanatkan dalam Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi dan tertuang dalam Penjelasan Umum Peraturan Pemerintah Republik Indonesia Nomor 52 Tahun 2000 Tentang Penyelenggaraan Komunikasi bahwa:

> "Penyelenggaraan jasa telekomunikasi diwajibkan untuk pertama, menyediakan fasilitas telekomunikasi yang menjamin adanya kualitas pelayanan jasa telekomunikasi yang baik. Kedua, penyelenggara jasa telekomunikasi dituntut untuk tidak bersikap diskriminatif dalam memberikan pelayanan kepada pengguna jasa telekomunikasi. Ketiga, penyelenggara jasa telekomunikasi diwajibkan untuk melakukan pencatatan/ perekaman pemakaian jasa telekomunikasi, serta wajib menyimpan catatan/rekaman dimaksud sekurang-kurangnya selama 3 (tiga) bulan."

Sejalan pula dengan pendapat yang diutarakan dalam hasil wawancara dengan Sutrisman selaku Direktur Eksekutif dari Asosiasi Penyelenggara Telekomunikasi Seluruh Indonesia (selanjutnya disebut ATSI) bahwa pada dasarnya penyelenggara jasa telekomunikasi memiliki 2 (dua) peran dalam keberlangsungannya yakni preventif dan represif. Fokus peran penyelenggara telekomunikasi dalam menanggulangi tindak pidana penipuan *online* saat ini lebih

[10] Di dalam melaksanakan *social engineering* inilah pelaku banyak menggunakan rangkaian kata bohong atau tipu muslihat, dalam istilah KUHP, dan berita bohong, dalam istilah UU ITE.

menekankan pada pencegahan (*preventif*). Hal ini disebabkan karena keberadaan daripada penyelenggara jasa telekomunikasi hanyalah sebatas menjadi alat trasnportasi berupa "pipa". Penyelenggara jasa telekomunikasi tidak dapat menyentuh isi dari pada informasi yang ada, melainkan hanya menjadi sebuah perantara untuk lalu lintas informasi tersebut. Sebagaimana telah dijelaskan dalam sub-bab sebelumnya mengenai prosedur standar penyelenggara jasa telekomunikasi bahwa langkah preventif yang dapat dilakukan oleh penyelenggara jasa telekomunikasi adalah meregistrasikan kartu perdana yang diedarkan dengan cara-cara yang telah ditetapkan dalam peraturan perundang-undangan yang ada. Setelah itu, data mengenai registrasi yang ada akan disimpan serta di verfikasi dan divalidasi oleh dinas kependudukan dan pencatatan sipil yang berwenang dalam hal tersebut. Dengan kewajiban registrasi Nomor MSISDN tersebut, dimaksudkan agar penipu tidak lagi memiliki sarana atau kesempatan yang dimanfaatkan untuk melakukan tindak pidana penipuan *online*.

Mengenai upaya penanganan represif, penyelenggara telekomunikasi bersedia bekerjasama. Perlu dipahami bahwa penanganan secara represif di sini maksudnya adalah dilakukan oleh penegak hukum. Apabila ada upaya represif oleh perseorangan, penyelenggara telekomunikasi tidak akan bekerjasama memberikan data apapun.

Selanjutnya dalam hal menjaga kerahasian data pelanggan oleh penyelenggara jasa telekomunikasi telah diatur dalam Pasal 40 hingga Pasal 42 Undang-Undang Nomor 36 Tahun 1999 Tentang Telekomunikasi:

> "Pasal 40
> Setiap orang dilarang melakukan kegiatan penyadapan atas informasi yang disalurkan melalui jaringan telekomunikasi dalam bentuk apapun.
>
> Pasal 41
> Dalam rangka pembuktian kebenaran pemakaian fasilitas telekomunikasi atas permintaan pengguna jasa telekomunikasi, penyelenggara jasa telekomunikasi wajib melakukan perekaman pemakaian fasilitas telekomunikasi yang digunakan oleh pengguna jasa telekomunikasi dan dapat melakukan perekaman informasi sesuai dengan peraturan perundang-undangan yang berlaku.

Pasal 42

(1) Penyelenggara jasa telekomunikasi wajib merahasiakan informasi yang dikirim dan atau diterima, oleh pelanggan jasa telekomunikasi melalui jaringan telekomunikasi dan atau jasa telekomunikasi yang diselenggarakannya.
(2) Untuk keperluan proses peradilan pidana, penyelenggara jasa telekomunikasi dapat merekam informasi yang dikirim dan atau diterima oleh penyelenggara jasa telekomunikasi serta dapat memberikan informasi yang diperlukan atas:
    a. permintaan tertulis Jaksa Agung dan atau Kepala Kepolisian Republik Indonesia untuk tindak pidana tertentu;
    b. permintaan penyidik untuk tindak pidana tertentu sesuai dengan Undang-undang yang berlaku.
(3) Ketentuan mengenai tata cara permintaan dan pemberian rekaman informasi sebagaimana dimaksud pada ayat (2) diatur dengan Peraturan Pemerintah."

Sutrisno kembali menekankan bahwa peran penyelenggara jasa telekomunikasi dalam menjaga kerahasian data pelanggan menjadi faktor yang sangat penting dalam hal penanggulangan tindak pidana penipuan secara *online,* hal ini disebabkan karena apabila kerahasian data pelanggan tersebut nyatanya tersebar baik karena kelalaian maupun karena disalahgunakan dari penyelenggara jasa telekomunikasi tentunya akan berakibat semakin luasnya terjadi tindak pidana penipuan *online* karena oknum-oknum tersebut dapat dengan bebasnya mengakses data pribadi seseorang yang kemudian digunakan sebagai modus penipuan.

Maka dari itu terdapat langkah-langkah yang dapat ditempuh apabila hendak mengakses data pribadi seseorang dalam sistem penyelenggara telekomunikasi harus menggunakan surat tertulis yang dikeluarkan oleh Badan Reserse Kriminal Mabes Polri atau *Monitoring Control* Mabes Polri. Sehingga badan lainnya yang berada di bawah Badan Reserse Kriminal Mabes Polri atau *Monitoring Control* Mabes Polri tidak memiliki kewenangan untuk mengakses data pribadi seseorang.

Di Pasal 41 Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi diatur bahwa penyelenggara telekomunikasi menyimpan rekaman konten komunikasi pengguna jasa telekomunikasi, untuk kepentingan pembuktian. Pada praktik umumnya, penyidik meminta rekaman tersebut selama tiga bulan terakhir.

Selain itu penyidik juga meminta data pelaku beserta alamat maupun pelacakan lokasi menggunakan *Base Transceiver Station* (selanjutnya disebut BTS). Kemudian penyidik akan meminta pendampingan penyelenggara jasa telekomunikasi ke lapangan ketika mendatangi lokasi hasil pelacakan karena penyelenggara jasa telekomunikasi yang mengetahui lokasi perkiraan yang terhubung dengan BTS. Peran penyelenggara jasa telekomunikasi upaya represif berhenti sampai di situ.

Prosedur pembukaan identitas pengguna kartu GSM prabayar dan hasil rekaman yang ada pada penyelenggara jasa telekomunikasi yang juga dapat dikatakan tidak praktis ini adalah sebagai upaya untuk mengeliminasi penyalahgunaan kewenangan terkait identitas pengguna jasa telekomunikasi dan data pribadi lainnya. Data pribadi dan hasil rekaman proses komunikasi tidak seharusnya disalahgunakan, oleh karenanya apabila orang lain ingin mengakses atau mendapatkannya, persyaratannya ketat. Mudahnya orang lain untuk mengakses atau mendapatkan identitas pengguna jasa telekomunikasi atau hasil rekaman komunikasinya dapat menyebabkan tingginya angka penyalahgunaan. Pembatasan itu memang penting, tetapi juga perlu dipikirkan jangan sampai pembatasan tersebut malah kontra-produktif dalam penegakan hukum.

Terpusatnya prosedur surat perintah pembukaan data pengguna jasa telekomunikasi dan informasi terkait pada Mabes POLRI membuat penyidik kepolisian daerah atau resort kota maupun sektor mengalami kendala. Bahkan dampaknya sampai pada persentase terpecahnya kasus yang masuk. Apabila semua surat perintah itu harus berpusat di Mabes POLRI, dan semua perkara penipuan online yang harus membuka data pelanggan dan informasi yang terkait seluruh Indonesia akan dimohonkan ke Mabes POLRI, belum lagi Mabes memiliki banyak kasus sendiri yang perlu ditangani. Dalam hal ini prinsip yang dianut mengutamakan perlindungan terhadap terjadinya penyalahgunaan, namun di saat yang sama juga mengakibatkan adanya inefisiensi kerja dalam penegakan hukum. Pencegahan penyalahgunaan data dan informasi pribadi mengalahkan kecepatan terselesaikannya kasus.

Hal ini sebenarnya juga sama dengan mekanisme pembukaan data nasabah perbankan dan simpanannya. Sehingga dapat dikatakan, hal tersebut yang dikemukakan di atas sebagai hal yang lumrah. Hal ini diatur dalam Undang-undang No. 7 Tahun 1992 Tentang Perbankan yang diubah dengan Undang-undang No. 10 Tahun 1998 tentang Perubahan Undang-undang No. 7 Tahun 1992 Tentang Perbankan (UU Perbankan). Pasal 1 angka 28 UU Perbankan, rahasia bank adalah segala sesuatu yang berhubungan dengan keterangan mengenai nasabah penyimpan dan simpanannya. Dari definisi tersebut, jelas kiranya bahwa yang diatur adalah rahasia bank terkait nasabah penyimpan. Termasuk keterangan mengenai nasabah penyimpan di bank, wajib dirahasiakan.

Pengecualian terhadap rahasia nasabah, atau dengan kata lain, rahasia nasabah boleh dibuka dengan syarat-syarat tertentu yang limitatif diatur dalam UU Perbankan dan Peraturan Bank Indonesia Nomor 2/19/PBI/2000 tentang Persyaratan dan Tata Cara Pemberian Perintah atau Izin Tertulis Membuka Rahasia Bank (PBI 2/19/2000). Yang salah satunya adalah untuk kepentingan peradilan dalam perkara pidana. Pimpinan Bank Indonesia dapat memberikan izin kepada Polisi, Jaksa, atau Hakim untuk memperoleh keterangan dari bank mengenai simpanan tersangka atau terdakwa pada bank (Pasal 42 ayat (1) UU Perbankan). Sedangkan teknisnya diatur dalam Pasal 6 PBI 2/19/2000, bahwa ijinnya diberikan atas permintaan tertulis dari Kepala Kepolisian Republik Indonesia, Jaksa Agung Republik Indonesia atau Ketua Mahkamah Agung Republik Indonesia. Selama ini penyidik mampu menyelesaikan perkara yang memerlukan pembukaan data nasabah perbankan dan simpanannya walaupun permohonan perijinan juga terpusat. Namun memang pada praktiknya, penyidik sudah memiliki banyak rekanan di sektor perbankan yang dapat memperlancar kinerja penegakan hukum, sedangkan di sektor telekomunikasi nampaknya masih belum.

Sampai saat ini masih belum ada pengaturan mengenai tindakan '*obstruction of justice*' yang subyeknya adalah penyelenggara jasa telekomunikasi secara khusus, yang tidak mau bekerjasama dalam penegakan hukum.

BAB V

SIMPULAN DAN SARAN

1. Simpulan

Peran penyelenggara jasa telekomunikasi dapat dibagi menjadi peran dalam upaya preventif dan peran dalam upaya represif. Mengenai upaya penanganan represif, penyelenggara telekomunikasi bersedia bekerjasama.

Sebenarnya tidak ada prosedur standar khusus mengenai penanganan penyalahgunaan penggunaan jasa telekomunikasi yang digunakan untuk menjalankan tindak pidana penipuan. Meksipun demikian, penyelenggara jasa telekomunikasi bersedia bekerja sama dengan penegak hukum, berdasarkan Peraturan Menteri Nomor 12 Tahun 2016.

Peran preventif letakknya pada mekanisme registrasi MSISDN. Proses registrasi sewaktu pengguna menginputkan NIK dan Nomor Kartu Keluarga, proses validasinya adalah *bypassing* ke dalam sistem elektronik milik Dinas Kependudukan dan Pencatatan Sipil. Kewajiban registrasi ini merupakan upaya untuk memberi ‘wajah’ pada setiap pengguna jasa telekomunikasi.

Dengan adanya proses registrasi, bukan berarti tindakan preventif sudah cukup untuk menekan agar jasa telekomunikasi tidak dijadikan sarana tindak pidana penipuan *online*. Pada dasarnya NIK dan Nomor KK sudah tersebar di mana-mana. Ketika nasabah bank mengajukan pinjaman atau kredit, kartu kredit, atau juga mendaftar sekolah atau kuliah, semua menggunakan KK yang juga terdapat NIK di dalamnya. Orang yang memiliki niat jahat bisa saja melakukan registrasi Nomor MSISDN dengan menggunakan NIK dan nomor KK orang lain, kemudian melaksanakan tindak pidana penipuan *online*. Hal itu merupakan pengaturan yang dapat mengeliminir kesempatan pelaku melakukan eksploitasi sarana yang dapat dilakukan untuk melakukan kejahatan.

Peran represif letaknya pada mekanisme penegakan hukum, yaitu pada tahap penyelidikan, penyidikan, dan pengadilan. Terdapat langkah-langkah

yang dapat ditempuh apabila hendak mengakses data pribadi seseorang dalam sistem penyelenggara telekomunikasi harus menggunakan surat tertulis yang dikeluarkan oleh Kapolri, dalam hal ini melalui Badan Reserse Kriminal Mabes Polri atau *Monitoring Control* Mabes Polri. Sehingga badan lainnya yang berada di bawah Badan Reserse Kriminal Mabes Polri atau *Monitoring Control* Mabes Polri tidak memiliki kewenangan untuk mengakses data pribadi seseorang. Penyelenggara telekomunikasi memiliki kewenangan memberikan rekaman konten komunikasi pengguna jasa telekomunikasi, untuk kepentingan pembuktian apabila ada surat dari Kapolri. Penyelenggara Jasa Telekomunikasi juga memiliki data pelaku beserta alamat maupun pelacakan lokasi menggunakan *Base Transceiver Station* (selanjutnya disebut BTS), dan dapat diberikan kepada penegak hukum berdasarkan surat yang dimaksud di atas.

2. Saran

Perlu diadakan penelitian tersendiri mengenai eliminasi ancaman penggunaan data pribadi berupa NIK dan Nomor KK. Selain itu perlu ada kriminalisasi tersendiri untuk penggunaan data pribadi secara melawan hukum, khususnya terkait NIK dan Nomor KK.

DAFTAR PUSTAKA

Buku

Chazawi, Adami dan Ardi Ferdian, *Tindak Pidana Informasi dan Transaksi Elektronik*, Media Nusa Creative: Malang, 2015

Bemmelen, J.M. van, *Hukum Pidana 3: Bagian khusus delik-delik khusus*, Binacipta: Bandung, 1986

Hamzah, Andi, *Delik-delik Tertentu (Speciale Delicten) di Dalam KUHP*, Sinar Grafika: Jakarta, 2014

Lamintang, P.A.F., *Dasar-dasar Hukum Pidana Indonesia*, Citra Aditya Bakti, Bandung, 1997

Lamintang, P.A.F. dan C. Djisman Samosir, *Delik-delik Khusus: Kejahatan yang Ditujukan Terhadap Hak Milik dan Lain-lain Hak yang Timbul dari Hak Milik*, Tarsito: Bandung, 1990

----------, *Hukum Pidana Indonesia*, cet. III, Sinar Baru: Bandung, 1990

Marpaung, Leden, *Asas Teori Praktik Hukum Pidana*, Sinar Grafika, Jakarta, 2005

Mertokusumo, Sudikno, *Mengenal Hukum: Suatu Pengantar*, Liberty: Jogjakarta, 2002

Moeljatno, *Fungsi dan Tujuan Hukum Pidana Indonesia*, Bina Aksara: Jogjakarta, 1985

Purwoleksono, Didik Endro, *Kapita Selekta Hukum Pidana*, Surabaya, 2010

Saleh, Roeslan, *Sifat Melawan Hukum Dari Perbuatan Pidana*, Aksara Baru: Yogyakarta, 1983

Soesilo, R.,*Kitab Undang-undang Hukum Pidana; Serta Komentar-komentarnya Lengkap Pasal Demi Pasal*, Politeia: Bogor, 1996

Tresna, R, *Azas-azas Hukum Pidana*, Pustaka Tinta Mas, 1994

Utrecht, E., *Hukum Pidana 1*, Pustaka Tinta Mas: Bandung, 1986

Penelitian

Anton Hendrik S. dan Andrian Julius, *Upaya Penanggulangan Tindak Pidana Penipuan Melalui Transaksi Jual Beli Online di Surabaya Dan Sekitarnya: Profil Modus Operandi Penipuan Melalui Transaksi Jual Beli Online yang Dilaporkan ke Reskrimsus Siber Polda Jatim*, Penelitian, LPPM Universitas Surabaya, 2016

Peraturan Perundang-undangan

Kitab Undang-undang Hukum Pidana

Undang-undang Nomor 36 Tahun 1999 tentang Telekomunikasi

Undang-Undang Nomor 2 Tahun 2002 Tentang Kepolisian Negara Republik Indonesia

Undang-undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-undang No. 19 Tahun 2016 tentang Perubahan Undang-undang No. 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 21 Tahun 2013 tentang Penyelenggaraan Jasa Penyediaan Konten pada Jaringan Bergerak Seluler dan Jaringan Tetap Lokal Tanpa Kabel dengan Mobilitas Terbatas

Peraturan Menteri Komunikasi dan Informatika Nomor 12 Tahun 2016 tentang Registrasi Pelanggan Jasa Telekomunikasi

Peraturan Pemerintah Republik Indonesia Nomor 52 Tahun 2000 Tentang Penyelenggaraan Komunikasi

LAMPIRAN 1

BIODATA KETUA PENELITI

I. IDENTITAS DIRI

I.1	Nama Lengkap (dengan gelar)	Anton Hendrik Samudra S.H., M.H.
I.2	Jabatan Fungsional	Dosen
I.3	NPK/NIDN	215020
I.4	Nomor HP	081931603030
I.5	Alamat Kantor	Fakultas Hukum Universitas Surabaya Raya Kalirungkut, Surabaya 60293
I.6	Nomor Telepon/Fax	0312981128
I.7	Alamat E-mail	antonhendrik@staff.ubaya.ac.id antonhendriks@yahoo.com
I.8	Mata Kuliah yang Diampu	- Kejahatan Siber - Kapita Selekta Hukum Pidana - Kejahatan Ekonomi - Kejahatan Transnasional

II. RIWAYAT PENDIDIKAN

Program	S-1	S-2	S-3
Ilmu Hukum (S.H.)	Fakultas Hukum Universitas Airlangga Surabaya (2003-2007)		
Magister Hukum (M.H.)		Magister Hukum Universitas Airlangga Surabaya (2010-2011)	
-			

III. PENGALAMAN PENELITIAN

No.	Tahun	Judul Penelitian	Sumber Pendanaan	
			Sumber	Jumlah
1.	2011	Asas Retroaktif dalam Pemberantasan Tindak Pidana Terorisme (Tesis)	-	
2.	2011	Penegakan Hukum Terhadap Tindak Pidana Penghinaan	-	

		Melalui Media Siber di Indonesia		
3.	2014	Kebebasan Atas Informasi dan Pembajakan Video, Musik, dan Software	-	
4.	2016	Upaya Penanggulangan Tindak Pidana Penipuan Melalui Transaksi Jual Beli Online di Surabaya Dan Sekitarnya: Profil Modus Operandi Penipuan Melalui Transaksi Jual Beli Online Yang Dilaporkan Ke Reskrimsus Siber Polda Jatim	LPPM Universitas Surabaya	Rp. 5.000.000,-

IV. PENGALAMAN PENGABDIAN KEPADA MASYARAKAT

No.	Tahun	Judul Pengabdian Kepada Masyarakat	Sumber Pendanaan	
			Sumber	Jumlah
1.	2013	Penyuluhan Hukum Tentang Bullying di SMP Kristen Gloria Kupang	Ubaya	Sesuai riil pengeluaran
2.	2015	Penyuluhan Hukum Tentang Bullying di SMA Kristen Gloria I Sukomanunggal	Ubaya	Sesuai riil pengeluaran
3.	2015	Penyuluhan Hukum Perlindungan Anak terkait ITE, SDK Cita Hati	FH Ubaya	Sesuai riil pengeluaran
4.	2016	Penyuluhan Hukum Perlindungan Anak terkait ITE, SDK Cita Hati	FH Ubaya	Sesuai riil pengeluaran
5.	2017	Penyuluhan Hukum dan Simulasi Persidangan kasus Perlindungan Anak terkait ITE, SDK Cita Hati	FH Ubaya	Sesuai riil pengeluaran

V. PENGALAMAN PENULISAN ARTIKEL ILMIAH DALAM JURNAL

No.	Tahun	Judul Artikel Ilmiah	Volume/Nomor	Nama Jurnal
1.	2017	Membanding Perbuatan yang Dilarang dalam UU ITE dan Konvensi Internasional:	Vol. 2, No. 1, Bulan Maret 2017, Penerbit: Program Studi Magister Ilmu	Jurnal Argumentum

		Penanggulangan Tindak Pidana Siber	Hukum Fakultas Hukum Universitas Surabaya	

VI. PENGALAMAN PENULISAN BUKU

No.	Tahun	Judul Buku	Jumlah Halaman	Penerbit
1.	2011	Prosiding Seminar Nasional *Soft Skill and Character Building*: Lintas Disiplin		Universitas Muhammadiyah, Surabaya
2.	2016	Prosiding International Conference on Financial Crimes	48 halaman	Kerjasama USDOJ, Universitas Surabaya, Universitas Thammasaat-Thailand
3.	2017	Tackling Financial Crimes: Various International Perspectives		Genta Publishing

VII. PENGALAMAN PEROLEHAN HKI

No.	Tahun	Judul/Tema HKI	Jenis	Nomor P/ID

VIII. PENGALAMAN MERUMUSKAN KEBIJAKAN PUBLIK/REKAYASA SOSIAL LAINNYA

No.	Tahun	Judul/Tema/Jenis Rekayasa Sosial yang Telah Diterapkan	Tempat Penerapan	Respon Masyarakat
1.	2017	Evaluasi Pemberantasan Tindak Pidana Korupsi: Penyadapan Dalam Penanggulangan Dan Penciptaan Budaya Anti-Korupsi	Rapat Kerja Kunjungan Spesifik Komisi III DPR ke Jawa Timur	Tanggapan Hakim-hakim positif, sedangkan DPR masih tetap pada agendanya

BIODATA ANGGOTA PENELITI

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	Dr. Go Lisanawati, S.H., M.Hum.
2	Jenis Kelamin	P
3	Jabatan Fungsional	Lektor (300)
4	NIP/NIK/Identitas Lainnya (NPK)	204023
5	NIDN	0723117702
6	Tempat dan Tanggal Lahir	Surabaya, 23 November 1977
7	E-mail	go_lisanawati@staff.ubaya.ac.id lisanawatigo@gmail.com
8	Nomor Telepon/HP	031-7662657/087859303821
9	Alamat Kantor	Raya Kalirungkut, Surabaya
10	Nomor Telepon/Faks	031-2981221/031-2981121
11	Lulusan Yang Telah Dihasilkan	S-1 = 25 orang
12	Mata Kuliah Yang Diampu	1. Hukum Pidana
		2. Kejahatan Ekonomi
		3. Kapita Selekta Hukum Pidana
		4. Kejahatan Siber

B. Riwayat Pendidikan

	S-1	S-2	S-3
Nama Perguruan Tinggi	Universitas Surabaya	Universitas Surabaya	Universitas Brawijaya
Bidang Ilmu	Ilmu Hukum	Ilmu Hukum	Ilmu Hukum
Tahun Masuk – Lulus	1996 – 2000	2000 – 2002	2006 – 2010
Judul Skripsi/Tesis/Disertasi	Perkawinan Anak Ditinjau Dari UU No. 1 Tahun 1974 Tentang Perkawinan	Pembagian Harta Kepailitan	Kebijakan Transfer Dana Elektronik dalam Tindak Pidana Pencucian Uang
Nama Pembimbing/Promotor	H. Heru Susanto dan Dr. J. M. Atik Krustiyati, S.H., M.S.	Prof. Dr. Erman Radjagugkguk, S.H., LL.M.	Prof. Dr. Hj. Made Sadhi Astuti, S.H Prof. Masruchin Ruba'i, S.H., M.S. Dr. Sarwirini, S.H., M.H.

C. Pengalaman Penelitian Dalam 5 Tahun Terakhir (Bukan Skripsi, Tesis, maupun Disertasi)

No	Tahun	Judul Penelitian	Pendanaan	
			Sumber*	Jumlah (Juta Rp)
1	2016	Model Pengaturan Partisipasi Profesi Hukum Dalam perundang-undangan Anti Pencucian Uang	DIKTI	65.000.000
2	2015	Implementasi Pembawaan Uang Tunai Dalam Perspektif Anti Pencucian Uang	LPPM	50.000.000
3	2012	*International Self Reported Delinquency*-3 (ISRD-3), kerjasama dengan University of Zurich, Switzerland	University of Zurich	390.000.000
4	2012	Fungsi *Social Reports* untuk Mewujudkan Sistem Peradilan Anak Yang Restoratif, kerjasama dengan Kementrian Hukum Dan Hak Asasi Manusia Kantor Wilayah Jawa Timur	Kanwil Hukum dan HAM Jawa Timur	10.000.000
5	2011	Anak dalam Dimensi Perlindungan Hukum Atas Kejahatan Siber	LPPM	12.310.000

D. Publikasi Artikel Ilmiah dalam Jurnal Dalam 5 Tahun Terakhir

No	Judul Artikel Ilmiah	Nama Jurnal	Volume/Nomor /Tahun
1	Telaah Atas eksistensi Lembaga Pengawas dan Pengatur Menurut UU Pencegahan dan pemberantasan Tindak Pidana Pencucian Uang, UU Bank Indonesia, dan UU Otoritas Jasa Keuangan	Buletin Hukum Perbankan dan Kebanksentralan	Volume 10, Nomor 1, Januari – April 2012

2	Penerapan Customer Due Diligence Atas Resolusi DK PBB Nomor 1267 Guna Pencegahan Tindak Pidanan Pendananan Terorisme	Buletin Hukum Perbankan dan Kebanksentralan	Volume 10, Nomor 3, September – Desember 2012
3	Aspek Perlindungan Data Privasi Dalam Perspektif Undang-UndangNomor 11 Tahun 2008	Yustika, UBAYA	Volume 15 No. 1 Juli 2012
4	Customer Due Diligence and Its Role to Prevent the Global Economic Threat: Indonesian Anti Money Laundering Perspective	South East Asian Journal of Business, Economic, and Law	2012
5	Cyber Child Sexual Exploitation dalam Perspektif Perlindungan atas Kejahatan Siber	Pandecta, Semarang	Vol 8 Nomor 1 Januari 2013
6	Pendidikan Tentang Pencegahan Kekerasan Terhadap Perempuan Dalam Dimensi Kejahatan Siber	Pandecta, Semarang	Vol 9 No. 1 Januari 2014
7	Anti Money Laundering Regime in Indonesia: Prevention and Eradication Perspectives	Thammasat Law Journal	Vol 43, No. 1, March 2014
8	The Issue of Freezing without delay in counter financing of terrorism and the implementation under Indonesian Law	Thammasat Law Journal	Vol 44 No 1, 2015
9	Best Principles for Criminal Assets Management: Conceptual Framework	UUM International Postgraduate Business Journal	Vol. 7(1), 2015
10	Why does New Payment System and Products (NPSPs) Vulnerable to Money Laundering?	Journal of Social and Developments Sciences	Vol 6, No. 3, 2015
11	What can IT and Money Laundering Law do to Fight against cyber child sexual crime?	Journal of Social and Developments Sciences	Vol. 6, No. 2, 2015
12	Legal Profession and Accountant Profession in the Turbulence of Money Laundering	IJABER	Vol 13 No. 5, 2015
13	Cash Courier in Money Laundering: Crime Opportunity Approach	Qualitative and Quantitative Research review	Vol 1 Issue 1, 2016

E. Pemakalah Seminar Ilmiah (Oral presentation) Dalam 5 Tahun Terakhir

No	Nama Pertemuan Ilmiah/Seminar	Judul Artikel Ilmiah	Waktu dan Tempat
1	Seminar "Pengembalian Aset Hasil Kejahatan dalam Perspektif Tindak Pidana Pencucian Uang"	Rezim Perampasan asset dalam Tindak Pidana Pencucian Uang	Universitas Internasional Batam, 28 Februari 2016
2	Rapat Kerja dan Seminar BKOW Provinsi Jawa Timur	Memahami Informasi dan Transaksi Elektronik melalui UU No. 11 Tahun 2008	BKOW Provinsi Jawa Timur, tanggal 17 November 2015
3	Diseminasi Draft Usulan Peraturan Pemerintah Tentang Pengendalian Gratifikasi	Urgensi Peraturan Pemerintah terkait pengendalian gratifikasi	Hotel Swissbel In, tanggal 13 November 2015
4	Diskusi Terbatas Rancangan Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana	Rancangan Undang-Undang Tentang Kitab Undang-Undang Hukum Pidana dalam perspektif Tindak Pidana Korupsi	Hotel Ibis, Jembatan Merah, 22 Oktober 2013
5	Seminar "Kejahatan Negara di Era Reformasi"	Tindak Pidana Pencucian Uang	Universitas Brawijaya, 30 Juni 2012
6	Sosialisasi mengenai Implementasi fungsi Social report dalam undang-undang nomor 3 Tahun 1997 tentang Pengadilan Anak	Fungsi Social Report dalam UU No. 3 Tahun 1997	Hotel Sinar, Juanda, Surabaya, 25 April 2012
7	Sosialisasi "Kita dan Sosial Media ditinjau dari UU ITE"	Sosial Media vs UU ITE	SD Kr Cita Hati, West Campus, 28 Januari 2012

F. Karya Buku Dalam 5 Tahun Terakhir

No	Judul Buku	Tahun	Jumlah Halaman	Penerbit
1	Problematika Pembaharuan Hukum Pidana Nasional	2013	378	Komisi Hukum Nasional (KHN)

2	Prosiding Seminar Nasional dan Call For Paper Korupsi dalam Kepelbagaian Interpretasi	2014	188	Universitas Satya Wacana, Salatiga
3	Prosiding Seminar Nasional dan Call for papers Refleksi 70 tahun Pembaharuan Hukum Pidana	2015		Universitas Semarang

G. Pengalaman Merumuskan Kebijakan Publik/Rekayasa Sosial Lainnya dalam 5 Tahun Terakhir

No	Judul/Tema/Jenis Rekayasa Sosial Lainnya Yang Telah Diterapkan	Tahun	Tempat Penerapan	Respon Masayarakat
1	Draft of Bill of Financing of Terrorism Draft RUU Pendanaan Terorisme Hasil dari Studi Ekskursi pada Australian Department of Justice	2012	PPATK bekerjasama dengan Dirjen Perundang-undangan RI	Telah Berlaku UU No. 9 Tahun 2013 tentang Pencegahan dan Pendanaan Terorisme
2	Rancangan KUHP dan Delik Korupsi dalam Sebuah Analisis	2014	Pertemuan Pakar Hukum Dalam Penyusunan Legal Opinion dan Upaya Advokasi RUU KUHAP dan KUHP	RUU KUHP dan RUU KUHAP ditunda diundangkan

H. Penghargaan dalam 10 Tahun Terakhir (dari Pemerintah, asosiasi atau institusi lainnya)

No	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun
1	Penghargaan 10 tahun kesetiaan	Universitas Surabaya	2014
2	Penghargaan Wisudawan Cumlaude	Universitas Brawijaya	2010

3	Penghargaan Wisudawan Terbaik	Program Pascasarjana Universitas Brawijaya	2010
4	Penghargaan Wisudawan Cumlaude	Universitas Surabaya	2002
5	Penghargaan Wisudawan Cumlaude	Universitas Surabaya	2000

BIODATA ASISTEN PENELITI

A. Identitas Diri

1	Nama Lengkap (dengan gelar)	Natalia Wijaya S.H.
2	Jenis Kelamin	P
3	Jabatan Fungsional	Mahasiswa
4	NPK/NIDN	120114040
5	Nomor HP	081217955979
6	Alamat E-mail	Nataliawijaya0106@gmail.com
7	Universitas	Universitas Surabaya
8	Alamat Universitas	Raya Kalirungkut, Surabaya

B. RIWAYAT PENDIDIKAN

Program	S-1	S-2	S-3
Ilmu Hukum (S.H.)	Fakultas Hukum Universitas Surabaya (2014-2018)		

C. Penghargaan dalam 5 Tahun Terakhir (dari Pemerintah, asosiasi atau institusi lainnya)

No	Jenis Penghargaan	Institusi Pemberi Penghargaan	Tahun
1	Penghargaan Wisudawan Cumlaude	Universitas Surabaya	2018
2	Penghargaan Wisudawan Terbaik	Universitas Surabaya	2018

D. PENGALAMAN PENELITIAN

No.	Tahun	Judul Penelitian	Sumber Pendanaan	
			Sumber	Jumlah
1.	2015	Perlindungan Konsumen Dalam Peredaran Obat dan Food Suplement	-	